

Study to support the preparation of an impact assessment on EU policy initiatives facilitating cross-border law enforcement cooperation

Final Report

Annex I

*Methodological approach and data basis of this study, overview of
existing EU measures & national rules on investigative tools*

October 2021

*This report has been prepared by EY and RAND Europe for the European Commission, Directorate-
General for Migration and Home Affairs.*

This study was carried out on behalf of the European Commission by



Main authors of the study

EY

- Katarina Bartz
- Nicoletta Colombo
- Ilia Gaglio
- Alana Gyszcas
- Florian Linz

RAND Europe

- Michaela Bruckmayer
- Emma Disley

European Commission

Directorate-General for Migration and Home Affairs

Study to support the preparation of an impact assessment on EU policy initiatives facilitating cross- border law enforcement cooperation

Final report

Annex I

*Methodological approach and data basis of this study, overview of
existing EU measures & national rules on investigative tools*

Europe Direct is a service to help you find answers to your questions about the European Union.

Freephone number (*):

00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

LEGAL NOTICE

This document has been prepared for the European Commission however it reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

More information on the European Union is available on the Internet (<http://www.europa.eu>).

Luxembourg: Publications Office of the European Union, 2021

PDF ISBN 978-92-76-43481-8
PRINT ISBN 978-92-76-43482-5

doi: 10.2837/07309
doi: 10.2837/90130

DR-01-21-418-EN-N
DR-01-21-418-EN-C

© European Union, 2021

Reproduction is authorised provided the source is acknowledged.

Table of Contents

1	OVERVIEW OF THE PROJECT TASKS AND ACTIVITIES	1
1.1	Preparatory phase	1
1.2	Phase 1 - Problem definition and design of the policy options.....	1
1.3	Phase 2 - Analysis of policy options	5
1.4	Assessment of the data collection process	6
2	EU MEASURES FOR CROSS-BORDER LAW ENFORCEMENT COOPERATION	7
2.1	Overview of EU relevant initiatives and related dimensions of analysis	8
2.2	Access to/exchange of information	9
2.3	Operational cooperation for public order and safety	15
2.4	Operational cooperation for SOC and terrorism	17
2.5	Data protection	25
2.6	EU Agencies' legal basis	26
3	NATIONAL RULES ON INVESTIGATIVE TOOLS USED TO FIGHT SERIOUS AND ORGANISED CRIME.....	29
4	COVERAGE OF ISSUES BY THE SCHENGEN EVALUATION REPORTS	321
5	CONSULTATION TOOLS AND STAKEHOLDERS ENGAGED	323
5.1	Consultation tools.....	323
5.2	List of stakeholders consulted	354
6	BIBLIOGRAPHY AND MAIN SOURCES OF INFORMATION	359
	EU Legal framework.....	359
	Information sharing	359
	Data protection	361
	EU Agencies.....	361
	Additional sources related to police cooperation.....	362
	Bi/Tri/Multilateral agreements.....	364
	Reports, studies, academic literature and other documentation	367

Table of Tables

Table 1 – Overview of the project tasks and activities for the preparatory phase.....	1
Table 2 – Overview of the project tasks and activities for Phase 1	1
Table 3 – Overview of the project tasks and activities for Phase 2	5
Table 4 – EU measures by dimension of analysis.....	8
Table 5 – Overview of binding EU measures with respect to the access to and exchange of information (Part 1).....	9
Table 6 – Overview of binding EU measures with respect to the access to and exchange of information (Part 2).....	11
Table 7 – Overview of non-binding EU measures with respect to the access to and exchange of information.....	12
Table 8 – Overview of binding EU measures with respect to operational cooperation for public order and safety	15
Table 9 – Overview of non-binding EU measures with respect to operational cooperation for public order and safety	16
Table 10 – Overview of binding EU measures with respect to operational cooperation for SOC and terrorism.....	17
Table 11 – Overview of non-binding EU measures with respect to operational cooperation for SOC and terrorism.....	18
Table 12 – Overview of EU measures focused on specific investigative tools - Controlled deliveries ...	19
Table 13 – Overview of EU measures focused on specific investigative tools – Hot pursuit.....	21
Table 14 – Overview of EU measures focused on specific investigative tools - Surveillance	23
Table 15 – Overview of EU measures focused on specific investigative tools – Covert investigations..	24
Table 16 – Overview of EU measures with respect to data protection.....	25
Table 17 – Overview of the legal basis of EU Agencies	26
Table 18 – Overview of national rules on investigative tools - Austria	29
Table 19 – Overview of national rules on investigative tools - Belgium.....	36
Table 20 – Overview of national rules on investigative tools - Bulgaria.....	52
Table 21 – Overview of national rules on investigative tools - Croatia	62
Table 22 – Overview of national rules on investigative tools - Cyprus	66
Table 23 – Overview of national rules on investigative tools - Czechia	71
Table 24 – Overview of national rules on investigative tools - Denmark	78
Table 25 – Overview of national rules on investigative tools - Estonia.....	84
Table 26 – Overview of national rules on investigative tools - Finland	89
Table 27 – Overview of national rules on investigative tools - France.....	97
Table 28 – Overview of national rules on investigative tools - Germany	124
Table 29 – Overview of national rules on investigative tools - Greece	130
Table 30 – Overview of national rules on investigative tools - Hungary	135
Table 31 – Overview of national rules on investigative tools - Iceland.....	149
Table 32 – Overview of national rules on investigative tools - Ireland	154
Table 33 – Overview of national rules on investigative tools - Italy.....	167
Table 34 – Overview of national rules on investigative tools - Latvia.....	174
Table 35 – Overview of national rules on investigative tools - Liechtenstein.....	180
Table 36 – Overview of national rules on investigative tools - Lithuania	186
Table 37 – Overview of national rules on investigative tools - Luxembourg.....	191
Table 38 – Overview of national rules on investigative tools - Malta	195
Table 39 – Overview of national rules on investigative tools - Netherlands	203
Table 40 – Overview of national rules on investigative tools - Norway	214
Table 41 – Overview of national rules on investigative tools - Poland.....	218
Table 42 – Overview of national rules on investigative tools - Portugal	234
Table 43 – Overview of national rules on investigative tools - Romania.....	240
Table 44 – Overview of national rules on investigative tools - Slovenia	254
Table 45 – Overview of national rules on investigative tools - Slovakia	292
Table 46 – Overview of national rules on investigative tools - Spain	301

Table 47 – Overview of national rules on investigative tools - Sweden	306
Table 48 – Overview of national rules on investigative tools - Switzerland.....	314
Table 49 – Overview of the extent to which the issues identified in the report are also reported in the Schengen Evaluation Reports	321
Table 50 – Survey questionnaire for LEAs	323
Table 51 – Overview of the interview guidelines for Phase 1	340
Table 52 – Guidelines for the case study interviews – Information Exchange	346
Table 53 – Guidelines for the case study interviews – Joint Operations	349
Table 54 – Guidelines for the case study interviews – Operational cooperation in relation to SOC and terrorism	351
Table 55 – Overview of potential impacts of the policy options.....	353
Table 56 – Overview of the number of stakeholders consulted from EU bodies.....	354
Table 57 – Overview of the number of stakeholders consulted from academia and think tanks	354
Table 58 – Overview of the number of stakeholders consulted from EMPACT Drivers	354
Table 59 – Overview of the number of stakeholders consulted from EMPACT Support Managers.....	355
Table 60 – Overview of the stakeholders consulted from LEAs	355
Table 61 – Overview of the stakeholders consulted from National Judicial Authorities	357
Table 62 – Overview of the stakeholders consulted from National Data Protection Authorities.....	357
Table 63 – Overview of the stakeholders consulted with respect to the Benelux Agreement.....	357
Table 64 – Overview of the stakeholders consulted with respect to the Czechia-Germany Agreement	358
Table 65 – Overview of the stakeholders consulted with respect to the France-Switzerland Agreement	358
Table 66 – Overview of the stakeholders consulted with respect to the Nordic Agreement.....	358
Table 67 – Overview of the stakeholders consulted as case studies	358

1 OVERVIEW OF THE PROJECT TASKS AND ACTIVITIES

1.1 Preparatory phase

Table 1 – Overview of the project tasks and activities for the preparatory phase

Activities	Status	Work conducted
P.1: Preliminary desk research and mapping of available data	Completed	- Mapping of relevant sources based on the list included in the Technical Proposal, the suggestions from DG HOME and stakeholders interviewed - Preliminary review of documents identified and creation of a catalogue that is kept progressively updated
P.2: Scoping interviews	Completed	Implementation of 7 scoping interviews (against the four initially foreseen) of the with relevant officials from the Commission (DG HOME, DG TAXUD and DG JUST).
P.3: First Law Enforcement Working Party meeting	Completed	The first Law Enforcement Working Party meeting took place on 16 March 2021. During this meeting the Team informed the relevant stakeholders about the project, illustrated the scope, objectives, methodological framework and timeline of the study and explained the related consultation plan.
P.4: Refinement of the analytical framework	Completed	Based on the results of the previous activities, the Team refined the analytical framework for Task 2 (analysis of EU and regional measures) and for Task 3 (analysis of national rules for investigative tools). The analytical framework also built on the feedback received by the Commission during the Kick-off Meeting (KoM).
P.5: Refinement of the data collection tools	Completed	- Identification and mapping of relevant stakeholders and identification of the focal points to be leveraged to reach out to stakeholders at the national level. The approach to stakeholder identification was discussed with the Commission during the KoM and was progressively updated based on feedback and indications received afterwards. - Refinement of the stakeholder consultation plan. - Drafting of consultation tools (i.e. questionnaire for the Public Consultation, questionnaires for the online survey addressing national stakeholders, guidelines for interviews with EU bodies and academia, guidelines for the focus groups on multilateral agreements).

Source: Author's own elaboration

1.2 Phase 1 - Problem definition and design of the policy options

Table 2 – Overview of the project tasks and activities for Phase 1

Activities	Status	Work conducted
Consultation activities		
Public consultation	Completed	- Upload of the questionnaire on Better Regulation Portal and implementation of tests. - The questionnaire has been sent to DG HOME in order to proceed with translation in all official languages recognised by the EU.

Activities	Status	Work conducted
		- Upload of the translated versions of the questionnaire on the Better Regulation Portal. - Analysis of the 20 replies after the PC is closed and integration of the Synopsis report with additional evidence.
Online survey	Completed	- The online survey was launched on 5 March 2021 via the EY eSurvey tool with the deadline set after four weeks (2 April 2021).¹ The survey was sent directly to DPAs, while for the other typologies of stakeholders the Team relied on a number of focal points, which acted as intermediaries between the Team and the different LEAs constituencies at the national level. - Three reminders were sent (19 March, 1 April and 20 April) and the deadline was extended to 30 April 2021. - Analysis of responses gathered and notably 239 responses: - o 216 from national LEAs' representatives; ▪ 46 from Specialised investigative Units; ▪ 33 from Experts from public safety/public order departments and National Football Information points (NFIP); ▪ 18 from Customs; ▪ 23 from SPOCs. ▪ 28 from Specialised Analytical Departments; ▪ 23 from PCCCs, ▪ 23 from National EMPACT Coordinators (NECs); ▪ 22 from national LEAs' representatives; - o 13 from national judicial authorities; - o 10 from national DPAs.
Interviews with EU bodies, academia and think tanks	Completed	Performance of 15 interviews (out of 17 initially planned)²: - 11 with EU bodies; - 4 with academia and think tanks. See Annex I.5.2 for a list of interviewees.
Focus groups with parties involved in the bi/tri/multilateral agreements	Completed	Performance of 4 focus groups with representatives from national LEAs involved in the implementation of four selected multilateral agreements: • Benelux agreement (Belgium, Netherlands, Luxembourg); • DE-CZ agreement; • CH-FR agreement; • Nordic countries agreement. See Annex I.5.2 for a list of participants.
Interviews with EMPACT actors	Completed	- Performance of 10 interviews with EMPACT drivers - Performance of 2 group interviews with EMPACT support managers
First technical workshop	Completed	The first technical workshop was organised by the Team and was held on 24 March 2021 via Webex. It lasted a full working day and involved an initial plenary session, three breakout sessions (corresponding to each of the problem drivers identified), and one final plenary session to discuss the findings of the different parallel breakout sessions. Representatives from DG HOME, DG JUST and the Council

¹ With the exception of the Data Protection Authorities that were contacted directly by the study team (27), all stakeholders have been addressed through their secretariats, which have disseminated the link to the online survey. Thus, no information on the exact number of recipients is available.

² Two additional follow-up interviews were performed with national representatives from LEAs.

Activities	Status	Work conducted
		participated in the meeting, as well as representatives from all EU Member States and two SACs.
Task 2: Provide a comparative overview of the cross-border law enforcement cooperation related measures/practices existing at EU and national levels including investigative tools		
Sub-task 2.1: Comparative overview of EU binding and non-binding acts	Completed	- Mapping of relevant EU measures (binding and non-binding) on intra-EU law enforcement cooperation and systematisation of information along a common framework of analysis (see Annex I.2) - Analysis of relevant documents (e.g. Schengen evaluation reports) including information on the implementation of EU measures at the national level and related challenges. - Comparative overview and analysis of coherence of EU measures to assess to what extent the different EU measures/practices considered are coherent in terms of focus and scope, and whether overlaps, discrepancies or gaps could be identified.
Sub-task 2.2: Thorough analysis of existing bi/tri/multilateral agreements implemented by Member States and Schengen Associated Countries	Completed	- Mapping of existing bi/tri/multilateral agreements and systematisation of information collected through the review of available agreements and relevant documents along a common framework of analysis (see Annex II) - Comparative analysis to identify commonalities and specificities - Identification of good practices and challenges based on specific selection criteria, including scope of application, administrative burden, etc. and on stakeholders' feedback
Task 3: Analyse if there is a need to harmonise investigative tools used to tackle and combat organised crime or a need for a minimum EU standard for organised crime investigations		
Sub-task 3.1: Mapping of the investigative tools to combat organised and serious international crime	Completed	- Analysis of national rules applicable to investigative tools to combat serious and organised crime in 26 Member States and SACs by the network of country correspondents and systematisation of the information collected through the review of national criminal codes and relevant case law along a common framework of analysis (see Annex I.3). - Comparative analysis of national rules to highlight common aspects and major differences with regard to the main investigative tools used to fight against serious and organised crime. - Analysis of national rules applicable to investigative tools to combat SOC in one Member State (BG).
Sub-task 3.2: Analysis of the use and effectiveness of investigative tools used by Member States	Completed	- Analysis of the survey responses received until 2 April and triangulation with stakeholder feedback gathered during interviews, focus groups and the workshop held on 24 March to assess the actual use and effectiveness of investigative tools - Finalisation of the analysis based on the full set of survey responses downloaded on 30 April 2020.
Sub-task 3.3: Analysis of the need for harmonisation of investigative tools or for an EU minimum standard	Completed	- Triangulation of evidence on the use and effectiveness of tools resulting from the previous sub-task with the analysis of the level of divergences among national laws resulting from sub-task 3.1 to assess the need for harmonisation for each of the main investigative tools. - Finalisation of the analysis based on the full set of survey responses to be downloaded on 30 April 2020.
Task 1: Define the problem at EU level and its possible evolution without further action at EU level		
Sub-task 1.1: Definition of the problem	Completed	- Analysis of all the evidence collected during the previous tasks and through stakeholder consultations to identify the high-level problems, the core problems and the related drivers to be addressed by the EU intervention and drafting of a summary problem tree.

Activities	Status	Work conducted
		- Identification of the relevant stakeholders concerned by the problems and how they are affected by them. - Refinement of some issues that need to be further substantiated through a limited number of short follow up interviews. - Integration of the problem definition with the analysis of the full set of survey responses. - See Annex I.4 for an overview of the coverage of the issues identified in the study by the Schengen Evaluation Reports and Annex I.6 for the bibliography and the list of the main sources of information used.
Sub-task 1.2: Analysis of the evolution of the problem	Completed	Analysis of the evolution of the high-level problems in the upcoming future without further EU intervention, by using as much as possible, qualitative and quantitative evidence.
Task 4: Justify whether EU action is required and appropriate, on the basis of legality, necessity, EU added value, and proportionality		
Sub-task 4.1: Analysis of subsidiarity	Completed	Analysis of the legal basis of the future EU intervention and assessment of the respect of the principle of subsidiarity through the performance of the necessity and EU added value test.
Sub-task 4.2: Analysis of proportionality	Completed	The analysis of proportionality was performed for the policy option 2 as preferred option for an EU intervention.
Task 5: Set out general and specific policy objectives and ensure these are consistent with other EU policies and objectives		
Sub-task 5.1: Identification of policy objectives	Completed	Design of policy objectives, addressing the problems and underlying drivers identified in Task 1. In particular, the policy objectives have been identified distinguishing between general and specific.
Sub-task 5.2: Assessment of consistency with the problems identified	Completed	Reconciliation of the identified problems with the policy objectives by means of a correspondence table. Such table represents in synthetic and diagrammatic way the links between the identified problems, and their drivers on the one hand, and the general and specific objectives on the other.
Sub-task 5.3: Assessment of consistency with the problems identified	Completed	Analysis of the consistency of the identified objectives (general and specific) with the EU acquis and other relevant EU policies and initiatives in the same policy area.
Task 6: Operational conclusions and recommendations on where clarification and improvement are potentially needed at EU level		
Sub-task 6.1: Elaboration of the baseline scenario and a long list of policy options	Completed	- Elaboration of the baseline scenario. - Development of a long list of legislative and non-legislative elements (or sub-options).
Sub-task 6.2: Preliminary screening of the possible policy options and sub-options	Completed	- Screening of the long list of legislative and non-legislative elements (or sub-options) in terms of feasibility and effectiveness. - Those elements for which a lack of feasibility was found were discarded for the policy options (see Annex IV for individual justification).
Sub-task 6.3: Identification and elaboration of a final list of policy options	Completed	- Clustering of the various retained sub-options to two policy options in addition to the baseline scenario, namely a legal proposal on minimum standards + supporting (soft) measures, legal proposal aiming for stronger alignment + supporting (soft) measures.

Source: Author's own elaboration

1.3 Phase 2 - Analysis of policy options

Table 3 – Overview of the project tasks and activities for Phase 2

Activities	Status	Work conducted
Consultation activities		
Case study interviews	Completed	Performance of twelve case study interviews with 26 representatives from Austria, France, Slovenia, Sweden and Switzerland. See Annex I.5.2 for a list of interviewees.
Interviews with EU bodies	Completed	Performance of eight interviews with 13 representatives from EU bodies. See Annex I.5.2 for a list of interviewees.
Second technical workshop	Completed	The second technical workshop was organised by the Team and was held on 25 May 2021 via Webex. The meeting focused on the development and validation of the policy options, as well as the assessment of their impacts. It lasted a full working day and involved an initial plenary session, three breakout sessions (corresponding to each of the core problems identified), and one final plenary session to discuss the findings of the different parallel breakout sessions. Representatives from DG HOME, DG JUST and the Council participated in the meeting, as well as representatives from all EU Member States and two SACs.
Task 7: Assess the impacts of the policy options		
Sub-task 7.1: Refinement of the impact assessment methodology	Completed	- Elaboration and fine-tuning of the approach for the impact assessment. - Selection of five case study countries for further interviews to analyse the likely impacts of the policy options elaborated. - Refinement and follow-up of specific issues that needed to be further addressed through a limited number of short follow up interviews.
Sub-task 7.2: Identification and preliminary assessment of likely impacts	Completed	- Preliminary assessment of the likely impacts of each policy option in order to screen the policy options for their most important types of likely impacts and to select the ones for a more detailed assessment.
Sub-task 7.3: In-depth qualitative and quantitative assessment of the impacts	Completed	- Detailed assessment of the likely impacts of each policy option in terms of effectiveness, efficiency, and coherence. - Performance of interviews in six case studies to analyse the likely impacts of the policy options elaborated, as well as with EU institutions. - Overall assessment of the likely impacts of each policy option in terms of security, economy, society, fundamental rights, and environment.
Task 8: Assess and rank the options on the basis of well-defined criteria, to be discussed with the Commission, and compare them to the baseline		
Sub-task 8.1: Comparison and ranking of the policy options	Completed	- Refinement of some methodological aspects such as ratings to be assigned, scale of ratings etc. - Comparison of the policy options as a whole against the baseline scenario. - Ranking of the performance of the policy options vis-à-vis the baseline scenario using a Multi-Criteria-Analysis.
Sub-task 8.2: Identification and assessment of the preferred policy option	Completed	- Selection and elaboration of the preferred policy option, including a detailed justification of the selection, a description of the main advantages/disadvantages, as well as a further assessment of its impacts.

Source: Author's own elaboration

1.4 Assessment of the data collection process

Overall, the **study involved the consultation of stakeholders at different levels of intervention**, notably:

- *EU Agencies, Bodies and Networks*: European Commission (Directorate-General for Migration and Home Affairs – DG HOME, Directorate-General for Taxation and Customs Union – DG TAXUD and Directorate-General for Justice and Consumers – DG JUST) and EU bodies with relevant expertise (the European Border and Coast Guard Agency (EBCGA/Frontex), the European Crime Prevention Network (EUCPN), the European Network on the Administrative Approach (ENAA), the European Union Agency for Criminal Justice Cooperation (Eurojust), the European Union Agency for Law Enforcement Cooperation (Europol), the European Public Prosecutor's Office (EPPO), the European Union Agency for Law Enforcement Training (CEPOL), the European Anti-Fraud Office (OLAF), the Fundamental Rights Agency (FRA), the European Data Protection Supervisor (EDPS), the European Judicial Network (EJN), the European Judicial Training Network (EJTN), and the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA).
- *National authorities*: National LEAs, national judicial authorities and national data protection authorities (DPAs);
- *Mixed EU level and national level stakeholders*: EMPACT – The European Multidisciplinary Platform Against Criminal Threats: Drivers and Support Managers of the different crime priorities addressed by the platform (involving actors from the two above categories);
- *Others*: Academia and think tank, as well as citizens.

The study encountered some difficulties, namely:

- **Sources were often inconclusive and made it difficult to properly substantiate certain issues.** While the analysis of the Schengen evaluation reports triangulated with the responses from the survey and the feedback gathered at the first technical workshop point at the existence of some issues, the documents often do not include enough detail to fully understand what the actual problematic aspects and their implications are. Similarly, stakeholders consulted, while confirming the existence of an issue, they often did not provide much factual evidence to allow a proper understanding of the critical aspects to be addressed. Also the feedback provided by stakeholders involved in the focus groups on the multilateral agreements was rather generic and not detailed enough to point at specific provisions that could be considered as a potential good practice and scaled up at an EU level.

Solution found: The Team further substantiated the existence of an issue by also relying on the Council documents and other studies that include recommendations to improve the same issue. The Team also performed a limited number of follow-up interviews with stakeholders that proved to be particularly engaged in the first project phase to collect anecdotal illustrative examples that might help better explain the issues identified as well as point at specific provisions of the multilateral agreements that could be considered when designing the policy options.

- **Feedback from stakeholders involved in the multilateral agreements remain quite generic and did not allow to identify specific provisions that could be taken as good practices.** Also the feedback provided by stakeholders involved in the focus groups on the multilateral agreements was rather generic and not detailed enough to point at specific provisions that could be considered as a potential good practice and included in the list of policy options.

Solution found: The Team performed a limited number of follow-up interviews with stakeholders that proved to be particularly engaged in the focus groups to further investigate at specific provisions of the multilateral agreements that could be considered when designing the policy options.

- **Stakeholders proved difficult to engage.** Despite the presentation of the consultation strategy at an early stage of the project by both the Team and the Commission at several instances, stakeholders proved difficult to engage. Some expressed concerns relating to the tightness of the deadline for completing the survey, since the information needed

required considerable time to be collected. Others required internal authorisations before giving their availability to discuss. Others needed several reminders before providing a response.

Solution found: The Team extended the duration of the survey (from 2 April to 30 April), thus allowing stakeholders more time to gather input and provide responses. Results and findings included in this report are therefore preliminary and will be integrated where needed with the full set of survey responses once the survey is closed.

The **quality of the information gathered is partially satisfactory** due to gaps in the evidence base and delays in stakeholder engagement.

2 EU MEASURES FOR CROSS-BORDER LAW ENFORCEMENT COOPERATION

This section includes the evidence collected to support Task 2. Information has been organised along five main dimensions of analysis:

- Access to/exchange of information;³
- Operational cooperation for public order and safety;⁴
- Operational cooperation for SOC and terrorism;⁵
- Data protection;
- EU Agencies' legal basis.⁶

With the exception of the latter two, each dimension of analysis is divided into two sub-sections encompassing binding and non-binding measure relevant for each dimension of analysis.

Finally, the dimension of analysis "Operational cooperation for SOC and terrorism" presents also an overview of the measures focused on specific investigative tools (i.e. controlled deliveries, hot pursuit, surveillance and covert investigations).

³ The following measures do not present information for this dimension: Council Document 13034/14 (Guidelines on the implementation of SFD); Council Document 6727/18 (Manual on Law Enforcement Information Exchange).

⁴ The following measures do not present information for this dimension: Council Decision 2008/616/JHA (Prüm Decision); Council Decision 2002/348/JHA concerning security in connection with football matches with an international dimension; Council Decision 2007/412/JHA concerning security in connection with football matches with an international dimension; Football Handbook (2006/C 322/01).

⁵ The following measures do not present information for this dimension: Council Decision 2009/917/JHA (Information technology for customs purposes); Council Document 10000/07 (European Union Manual: Traces on the Ownership of Firearms); Council document 15429/16 (Handbook for the Naples II Convention); Council Document 10590/18 (Guidance on the Naples II Convention).

⁶ The following measure does not present information for this dimension: Regulation 2018/1726 (eu-LISA).

2.1 Overview of EU relevant initiatives and related dimensions of analysis

Table 4 – EU measures by dimension of analysis

Measure	Dimensions of analysis		
	Access to/exchange of information	Public order and safety	SOC and terrorism
Binding measures			
CISA 1990			✓
Convention on mutual assistance and cooperation between customs administrations (Naples II Convention) - OJ C 24 1998	✓		✓
Council Decision 2002/348/JHA concerning security in connection with football matches with an international dimension	✓	✓	
Council Decision 2005/671/JHA on the exchange of information and cooperation concerning terrorist offences	✓		✓
Council Decision 2006/560/JHA of 24 July 2006 amending Decision 2003/170/JHA on the common use of liaison officers posted abroad by the law enforcement agencies of the Member States	✓		✓
Council Decision 2007/412/JHA concerning security in connection with football matches with an international dimension	✓	✓	
Council Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime	✓	✓	✓
Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime	✓	✓	✓
Council Decision 2008/617/JHA on the improvement of cooperation between the special intervention units of the Member States in crisis situations		✓	✓
Council Decision 2008/633/JHA concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences	✓		✓
Council Decision 2009/917/JHA on the use of information technology for customs purposes	✓		✓
Council Framework Decision 2006/960/JHA on simplifying the exchange of information and intelligence (SFD)	✓		✓
Regulation (EU) 2018/1860 on the use of the SIS for the return of illegally staying third-country nationals	✓	✓	✓
Regulation (EU) 2018/1861 on the establishment, operation and use of the SIS in the field of border check	✓	✓	✓
Regulation (EU) 2018/1862 on the establishment, operation and use of the SIS in the field of police cooperation	✓	✓	✓
Regulation (EU) 2019/818 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration	✓		✓
Non-binding measures			
Commission Recommendation (EU) 2017/820 on proportionate police checks and police cooperation in the Schengen area		✓	✓
Council Document 10000/07 - Proposal for a Council Recommendation on a standard procedure in Member States for cross-border enquiries by police authorities in investigating supply channels for seized or recovered crime-related firearms	✓		✓
Council Document 9512/10 - Guidelines on the implementation of Council Framework Decision 2006/960/JHA	✓	✓	
Council Document 15785/3/10 - Updated Catalogue of Recommendations for the correct application of the Schengen Acquis and Best practices: Police cooperation		✓	✓
Council Document 9105/11 - PCCCs guidelines	✓		✓
Council Document 6721/3/14 - Draft SPOC Guidelines for international law enforcement information exchange	✓		✓
Council Document 10492/14 - Guidelines for a SPOC	✓	✓	✓
Council Document 13034/14 - Guidelines on the implementation of SFD	✓		✓
Council Document 15429/16 - Handbook for the Naples II Convention			✓
Council Document 5825/20, 2 December 2020 (Manual on Law Enforcement Information Exchange)	✓	✓	✓
Council Document 10590/18 - Guidance on the Naples II Convention			✓
Council Document 13887/20 - Manual on cross-border operations		✓	✓
Council Resolution concerning an updated handbook with recommendations for international police cooperation and measures to prevent and control violence and disturbances in connection with football matches with an international dimension (2006/C 322/01- Football Handbook)	✓	✓	
Data Protection (binding)			
Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector	✓	✓	✓
Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data	✓	✓	✓

Measure	Dimensions of analysis		
	Access to/exchange of information	Public order and safety	SOC and terrorism
Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data	✓	✓	✓
Regulation (EU) 2018/1725 on the processing of personal data by the Union institutions, bodies, offices and agencies	✓	✓	✓
EU Agencies' legal basis (binding)			
Regulation (EU) 2015/2219 of the European Parliament and of the Council of 25 November 2015 on CEPOL	✓	✓	✓
Regulation (EC) No 1920/2006 on EMCDDA	✓		✓
Regulation (EU) 2016/794 on Europol	✓		✓
Regulation (EU) 2018/1726 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA)	✓	✓	✓
Regulation (EU) 2018/1727 on Eurojust	✓		✓
Regulation (EU) 2019/1896 on EBCGA	✓	✓	✓

2.2 Access to/exchange of information

Binding

2.2.1.1 Binding I

Table 5 – Overview of binding EU measures with respect to the access to and exchange of information (Part 1)

	Council Decision 2006/560 on the common use of liaison officers posted abroad	Council Decision 2008/633 (VIS for terrorist offences and of other serious criminal offences)	Council Framework Decision 2006/960 (SFD)	Regulation 2018/1860 (SIS II) Regulation 2018/1861 (SIS II) Regulation 2018/1862 (SIS II)	Regulation 2019/818 (Interoperability between EU information systems)
Objective	To ensure that Europol's liaison officers seconded to third countries and international organisations provide it with information relating to serious threats of criminal offences to Member States for those criminal offences for which Europol is competent under the Europol Convention	To provide access to Member States' designated authorities and the European Police Office (Europol) for consultation of the Visa Information System (VIS) for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences	To establish the rules under which Member States' law enforcement authorities may exchange information and intelligence effectively and expeditiously for the purpose of conducting criminal investigations or criminal intelligence operations	• <u>Regulation 2018/1860 (SIS II)</u>: to strengthen enforcement of the EU's return policy and reduces incentives for illegal immigration into the EU. • <u>Regulation 2018/1861 (SIS II)</u>: to define the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement. • <u>Regulation 2018/1862 (SIS II)</u>: to define the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters	To establish a European search portal (ESP) for the purposes of facilitating the fast, seamless, efficient, systematic and controlled access of Member State authorities and Union agencies to the EU information systems
Type of information to be exchanged	Serious threats of criminal offences	VIS data (personal data, travel data)	Information and intelligence referred to any type of information or data held by Law Enforcement Authorities (LEAs) or held by public authorities/private entities and which is available to LEAs without the use of coercive measures.	Personal data and supplementary information	Personal data and travel documents
Tools/ information systems used to exchange information		Substantiated request in written or electronic form	• Annex A includes a form to be used by the requested Member State in case of transmission/delay/ refusal of information	SIS	ESP

	Council Decision 2006/560 on the common use of liaison officers posted abroad	Council Decision 2008/633 (VIS for terrorist offences and of other serious criminal offences)	Council Framework Decision 2006/960 (SFD)	Regulation 2018/1860 (SIS II) Regulation 2018/1861 (SIS II) Regulation 2018/1862 (SIS II)	Regulation 2019/818 (Interoperability between EU information systems)
			Annex B: request form for information and intelligence to be used by the requesting member state		
Specific actors involved in the exchange of information	Europol liaison officers	Designated authorities of Member States	Competent law enforcement authority; Competent Prosecutor/Judicial authority	Sirene Bureau	Member State authorities and EU agencies having access to, at least, one of the EU information systems. Queries to the Common Identity Repository (CIR) shall be carried out by a police authority
Timing for exchanging information		Immediately and, in any case, no later than 60 days	Urgent request of information or intelligence held in a database directly accessible by a law enforcement authority: 8 hours (able to be postponed to maximum 3 days); Non urgent request of information or intelligence referred to the crimes above, held in a database directly accessible by a law enforcement authority: 1 week; Other cases: within 14 days		
Language to be used for the exchange of information			Language applicable for the channel used		
Requirements for exchanging information relating to specific areas		Two requirements are necessary: Access for consultation must be necessary for the purpose of the prevention, detection or investigation of terrorist offences or other serious criminal offences; There are reasonable grounds to consider that consultation of VIS data will contribute to the prevention, detection or investigation of a criminal offence			
Mechanisms to ensure Data Protection when accessing/exchanging information		Each Member State shall adopt the necessary security measures with respect to data to be retrieved from the VIS pursuant to this Decision and to be subsequently stored	Usage of channels for international law enforcement cooperation without any further specification	Member States shall ensure that the independent supervisory authorities designated in each Member State monitor the lawfulness of the processing of personal data in SIS on their territory, its transmission from their territory and the exchange and further processing of supplementary information on their territory	Biometrical templates shall be stored in the shared BMS only for as long as the corresponding biometric data are stored in the CIR or SIS. Common identity data shall be deleted from the CIR in an automated manner in accordance with the data retention provisions of Regulation (EU) 2019/816
Requirement to develop cross-border threat assessment/risks analysis					

Source: Author's own elaboration

2.2.1.2 Binding II

Table 6 – Overview of binding EU measures with respect to the access to and exchange of information (Part 2)

	Council Decision 2005/671 (exchange of information and cooperation concerning terrorist offences)	Council Decision 2008/615/JHA (Prüm Decision)	Council Decision 2002/348/JHA concerning security in connection with football matches with an international dimension	Council Decision 2007/412/JHA concerning security in connection with football matches with an international dimension	Council Decision 2009/917 (Information technology for customs purposes)	Naples II Convention
Objective	To share information with Europol, Eurojust and Member States	To improve cross-border cooperation and exchange of information between authorities responsible for the prevention and investigation of criminal offences	To prevent and combat football-related violence	The measure provides some amendments to the Decision 2002/348/JHA concerning security in connection with football matches with and international dimension	To establish Customs Information System; To establish customs files identification database	To provide information which may enable the requesting Member State to prevent, detect and prosecute infringements
Type of information to be exchanged	Personal data, relevant information concerning and resulting from criminal investigations conducted by LEAs with respect to terrorist offences which affect or may affect two or more Member States	Personal data and information	Personal data	Strategic operational and tactical information	Personal data and all data useful to achieve the objective in the following categories: Commodities; Means of transport; Businesses; Persons; Fraud trends; Availability of expertise; Items detained, seized or confiscated; Cash detained, seized or confiscated. No items of personal data shall be entered in any event within the category "fraud trends"	
Tools/ information systems used to exchange information				Information shall be exchanged using the appropriate forms contained in the appendix to the Football Handbook (2006/C 322/01)	Customs Information System (established for the purpose)	
Specific actors involved in the exchange of information		Specific National Contact Point (NCP)	National football information point (NFIP)	NFIP and competent authorities in Member States	Direct access to data entered into the Customs Information System shall be reserved to customs administrations, but may also include other authorities competent, according to the laws, regulations and procedures of the specific Member State	Customs authorities
Timing for exchanging information						
Language to be used for the exchange of information			National language. Translation in a working language common to both sides should be used	National language. Translation in a working language common to both sides should be used		Requests shall be submitted in an official language of the Member State of the requested authority or in a language acceptable to such authority
Requirements for exchanging information relating to specific areas			Public order purpose (preventing and combating football-related violence)		Personal data may be entered into the Customs Information System only if there are real indications, in particular on the basis of prior illegal activities, to suggest that the person concerned has committed, is in the act of committing or will commit serious contraventions of national laws	Request shall include: The applicant authority making the request; The measure requested; The object of, and the reason for, the request; the laws, rules and other legal provisions involved; Indications on the natural or legal persons being the target of the investigation;

	Council Decision 2005/671 (exchange of information and cooperation concerning terrorist offences)	Council Decision 2008/615/JHA (Prüm Decision)	Council Decision 2002/348/JHA concerning security in connection with football matches with an international dimension	Council Decision 2007/412/JHA concerning security in connection with football matches with an international dimension	Council Decision 2009/917 (Information technology for customs purposes)	Naples II Convention
						A summary of the relevant facts
Mechanisms to ensure Data Protection when accessing/exchanging information		The level protection of personal data at the national level should at least be equal to that resulting from the Council of Europe Convention for the Protection of Individuals and its Additional Protocol	Personal data shall be exchanged in accordance with the domestic and international rules applicable and using the appropriate forms contained in the appendix to the Football Handbook (2006/C 322/01)		Data entered into the Customs Information System shall be kept only for the time necessary to achieve the purpose for which they were entered. The need for their retention shall be reviewed at least annually by the supplying Member State	The customs authorities shall take into account in each specific case the requirements for the protection of personal data. They shall respect the relevant provisions of the Convention of the Council of Europe of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data
Requirement to develop cross-border threat assessment/risks analysis			NFIP should provide at the request of another NFIP a risk assessment of their own country's clubs and national team			

Source: Author's own elaboration

Non-binding

Table 7 – Overview of non-binding EU measures with respect to the access to and exchange of information

	Council Document No 9512/10 (Guidelines on the implementation of SFD)	Council Document 10492/14 (Guidelines for SPOC)	Council Document 6721/3/14 (SPOC guidelines)	Council Document 13034/14 (Guidelines on the implementation of SFD)	Council Document No 5825/20 (Manual on Law Enforcement Information Exchange)	Council Document No 9105/11 (PCCCs guidelines)	Football Handbook (2006/C 322/01)
Objective	To enhance the effective and expeditious exchange of information and intelligence between law enforcement authorities	To provide guidelines for SPOC for which SPOC should access, directly or at request from competent authorities, to the broadest range of relevant national databases and in any case to all those databases available to the authorities represented in the SPOC	To provide guidelines for SPOC for which SPOC should access, directly or at request from competent authorities, to the broadest range of relevant national databases and in any case to all those databases available to the authorities represented in the SPOC			To provide guidelines for PCCCs for which PCCCs should act as a "facilitator" of information exchange between States.	To provide a Handbook helping NFIP coordinating the exchange of information on football matches. The NFIP should contribute to public order, peace and safety, thus aiming at an efficient use of the available resources. The NFIP should also aim to facilitate international police cooperation regarding the police approach to the football issues and to promote the exchange of information between the police services of the different countries
Type of information to be exchanged	Any type of information or data which is held by law enforcement authorities, public authorities or by private entities and which is available to law enforcement authorities without the taking of coercive measures	Any type of information contained in law enforcement databases, identity documents database, visa database, immigration office database, prisoners database, information exchange with the national liaison officers, border control database	Any type of information contained in law enforcement databases, identity documents database, visa database, immigration office database, prisoners database, information exchange with the national liaison officers, border control database			Information related to petty and moderately serious crime, illegal migration flows and public order problems	General and personal information

	Council Document No 9512/10 (Guidelines on the implementation of SFD)	Council Document 10492/14 (Guidelines for SPOC)	Council Document 6721/3/14 (SPOC guidelines)	Council Document 13034/14 (Guidelines on the implementation of SFD)	Council Document No 5825/20 (Manual on Law Enforcement Information Exchange)	Council Document No 9105/11 (PCCCs guidelines)	Football Handbook (2006/C 322/01)
Tools/ information systems used to exchange information	Annex A :form to be used by the requested Member State in case of transmission/delay/refusal of information; Annex B: request form for information and intelligence to be used by the requesting Member State	SIS, CIS SIENA, Interpol (I-24/7 communication system), and TESTA-NG	SIS, CIS and TESTA-NG			Secure internal and external communications system, (e.g. systems similar to those employed by the national operational agencies - telephony, fax, e-mail, etc.). To increase efficiency and budgetary rationality, each PCCC party should be able to use a national line to communicate with its home country agencies and authorities. Dedicated software should be installed in order to facilitate the circulation of information within the PCCC in real time and to ensure daily recording and fast processing of questions referred to it and standardised recording of statistics	
Specific actors involved in the exchange of information	Police, customs and other authority authorised by national law to detect, prevent and investigate offences or criminal activities	SPOC Judicial authorities (when appropriate)	Europol, Interpol, SIRENE			PCCCs and Member States national agencies	Liaison officers, national football information point; for international tournaments, the formal request for support should come from the minister of the department responsible in the organising country, who will receive advice from the NFIP concerned
Timing for exchanging information		All databases are accessible to the unit on a 24/7 basis, where necessary via on-call duty officers					
Language to be used for the exchange of information	Member State language						The national language can be used for the communication between the different NFIPs if a copy of it is provided in the working language common to the two parties (unless other arrangements have been made between the parties concerned)
Requirements for exchanging information relating to specific areas	Requests and answers exchanged shall always provide Europol in copy each time that the request falls under Europol's mandate		A request is sent through one channel only and if it is sent through different channels at the same time, this is clearly indicated. The channel is not be changed during an on-going operation or during any phase unless it is				Public order purpose (preventing and combating football-related violence)

	Council Document No 9512/10 (Guidelines on the implementation of SFD)	Council Document 10492/14 (Guidelines for SPOC)	Council Document 6721/3/14 (SPOC guidelines)	Council Document 13034/14 (Guidelines on the implementation of SFD)	Council Document No 5825/20 (Manual on Law Enforcement Information Exchange)	Council Document No 9105/11 (PCCCs guidelines)	Football Handbook (2006/C 322/01)
			absolutely necessary and the partner's choice of channel when replying to the requests is respected. A change of channel is communicated to all parties, including the reason for the change. The purposes of and restrictions on the processing of information defined by the provider of the information are respected. Whenever possible, the SPOC replies directly to the international request, where appropriate with copy to the concerned national authority. Where the SPOC cannot reply directly, it forwards the request to the appropriate competent national authority, even if the original request was wrongly addressed to another authority. When a request is refused, the grounds for refusal have to be provided through the initial channel. When receiving a reply from the national authorities to an international request, the unit proactively verifies whether this information can be useful to another Member State, Europol or Eurojust and if this is the case, requests and encourages the owner of the information to transmit the information further				
Mechanisms to ensure Data Protection when accessing/exchanging information		The SPOC shall respect all applicable data protection rules	The SPOC shall respect all applicable data protection rules			The exchange of information must comply with current data protection and data dissemination provisions in the respect of the national legislation	In accordance with the applicable national and international legislation, the NFIP should be responsible for administering the personal data regarding risk supporters
Requirement to develop cross-border threat assessment/risks analysis							With regard to football matches with an international dimension, it is necessary that the NFIP has at its disposal, for the benefit of the NFIPs of the other countries, an updated risk-analysis

	Council Document No 9512/10 (Guidelines on the implementation of SFD)	Council Document 10492/14 (Guidelines for SPOC)	Council Document 6721/3/14 (SPOC guidelines)	Council Document 13034/14 (Guidelines on the implementation of SFD)	Council Document No 5825/20 (Manual on Law Enforcement Information Exchange)	Council Document No 9105/11 (PCCCs guidelines)	Football Handbook (2006/C 322/01)
							related to its own clubs and its national team

Source: Author’s own elaboration

2.3 Operational cooperation for public order and safety

Binding

Table 8 – Overview of binding EU measures with respect to operational cooperation for public order and safety

	Council Decision 2008/615/JHA (Prüm Decision)	Council Decision 2008/616/JHA (Prüm Decision)	Council Decision 2008/617/JHA (special intervention units)	Council Decision 2002/348/JHA concerning security in connection with football matches with an international dimension	Council Decision 2007/412/JHA concerning security in connection with football matches with an international dimension
Objective	To help Member States in the prevention of terrorist offences. Member States may, in individual cases, even without being requested to do so, supply other Member States' national contact points with personal data and information in so far as is necessary because particular circumstances give reason to believe that the data subjects will commit criminal offences related to terrorism		To improve cooperation between Member States' special intervention units in man-made crisis situations that present a serious and direct physical threat. The Decision establishes the general rules and conditions for the provision of assistance by these units to any requesting Member State.		
Specific situation critical for public order	Ensure security in mass events, health crisis, disaster, serious accidents		Crisis situation		
Type of law enforcement cooperation activity concerned	Intelligence/information sharing, joint operations, joint patrols		Special intervention unit		
Stakeholders involved	Police officers		Competent authorities of Member States		
Main features of the cooperation activity	A host Member State may confer executive powers on the seconding Member States' officers involved in joint operations or allow the seconding Member States' officers to exercise their executive powers in accordance with the seconding Member State's law, under the guidance and, as a rule, in the presence of officers from the host Member State Officers from a seconding Member State who are involved in a joint operation within another Member State's territory may wear their own national uniforms there. They may carry such arms, ammunition and equipment as they are allowed to under the seconding Member State's national law. The host Member State may prohibit the carrying of		Through a request via the competent authorities setting out the nature of the assistance requested and the operational necessity, a Member State may ask to be assisted by a special intervention unit of another Member State with a view to dealing with a crisis situation. The competent authority of the requested Member State may accept or refuse such a request or may propose a different kind of assistance		

	Council Decision 2008/615/JHA (Prüm Decision)	Council Decision 2008/616/JHA (Prüm Decision)	Council Decision 2008/617/JHA (special intervention units)	Council Decision 2002/348/JHA concerning security in connection with football matches with an international dimension	Council Decision 2007/412/JHA concerning security in connection with football matches with an international dimension
	particular arms, ammunition or equipment				
Criteria for developing joint operations					
Specific requirements for the use of arms/equipment	Officers may carry arms, ammunition and equipment as they are allowed to under the seconding Member State's national law. The host Member State may prohibit the carrying of particular arms, ammunition or equipment				
Requirements relating to Data Protection	Each Member State shall guarantee a level of protection of personal data in its national law at least equal to that resulting from the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its Additional Protocol		Data protection are not collected		
Requirement to develop cross-border threat assessment/risks analysis					

Source: Author’s own elaboration

Non-binding

Table 9 – Overview of non-binding EU measures with respect to operational cooperation for public order and safety

	Commission Recommendation (EU) 2017/820 on proportionate police checks and police cooperation in the Schengen area	Football Handbook (2006/C 322/01)
Objective	To remedy the threats to public policy or internal security within the Schengen area	
Specific situation critical for public order		
Type of law enforcement cooperation activity concerned	Police checks on the territory on transport routes and in border areas. Use of modern technologies to monitor vehicles and traffic flows	
Stakeholders involved	Police and custom authorities	
Main features of the cooperation activity	To strengthen cross-border police cooperation in addressing threats to public policy or internal security, Member States should: Re-assess the extent to which they currently use all available cross-border police operational cooperation tools such as joint patrols, joint operations, joint investigation teams, cross-border hot pursuits, or cross-border surveillances, PCCCs; Work jointly with their neighbouring Member States to remove legal or operational barriers to the full use of all cross-border operational police cooperation tools; Develop and implement, as appropriate, joint threat analysis and cross-border information exchanges with their neighbouring Member States to support joint actions to address threats to public policy or internal security in shared internal border areas, including through coordinated police checks in their internal border areas; Assess the need for technical investments to enhance joint operations, notably for surveillance and detection	
Criteria for developing joint operations		

	Commission Recommendation (EU) 2017/820 on proportionate police checks and police cooperation in the Schengen area	Football Handbook (2006/C 322/01)
Specific requirements for the use of arms/equipment		
Requirements relating to Data Protection		
Requirement to develop cross-border threat assessment/risks analysis		

Source: Author’s own elaboration

2.4 Operational cooperation for SOC and terrorism

Binding

Table 10 – Overview of binding EU measures with respect to operational cooperation for SOC and terrorism

	Council Decision 2008/615/JHA (Prüm Decision)	Convention implementing the Schengen Agreement (CISA)	Naples II Convention	Council Decision 2009/917/JHA (Information technology for customs purposes)
Objective	To help Member States in the prevention of terrorist offences. Member States may, in individual cases, even without being requested to do so, supply other Member States' national contact points with personal data and information in so far as is necessary because particular circumstances give reason to believe that the data subjects will commit criminal offences related to terrorism		To provide some provisions on criminal law enforcement cooperation for customs authorities. The Convention enables central coordinating units appointed within each national customs authority to exchange requests (in principle in writing) for information, surveillance, and enquiries. Moreover, the Convention establishes that customs authorities must provide each other with the necessary staff and organisational support when cooperating on cross-border issues	
Relevant crime area	Terrorism, cross border crimes		Traffic of drugs and psychotropic substances, weapons, munitions, explosive materials, cultural goods, dangerous and toxic waste, nuclear material or materials or equipment intended for the manufacture of atomic, biological and/or chemical weapons (prohibited goods); Trade in narcotic drugs and psychotropic substances and intended for the illegal manufacture of drugs (precursor substances); trade in taxable goods to evade tax or to obtain unauthorised State payments in connection with the import or export of goods, trade in goods prohibited	
Type of law enforcement cooperation activity concerned	Intelligence/information sharing, joint operations, joint patrols	Intelligence/information sharing	Joint operations	
Main features of the cooperation activity	Notifying one another as promptly as possible of situations with a cross-border impact and exchanging any relevant information; Taking and coordinating the necessary policing measures within their territory in situations with a cross-border impact; Dispatching officers, specialists and advisers and supplying equipment, at the request of the Member State within whose territory the situation has arisen		The participating authorities shall apply to their judicial authorities for approval of the planned investigations. Information obtained by officers during cross-border cooperation may be used, in accordance with national law and subject to particular conditions laid down by the competent authorities of the State in which the information was obtained, as evidence by the competent bodies of the Member State receiving the information. Requests for assistance shall always be made in writing	
Stakeholders involved	Police, Member States contact points		Customs authorities	

	Council Decision 2008/615/JHA (Prüm Decision)	Convention implementing the Schengen Agreement (CISA)	Naples II Convention	Council Decision 2009/917/JHA (Information technology for customs purposes)
Criteria for developing joint operations				
Specific requirements for the use of arms/equipment	Officers may carry arms, ammunition and equipment as they are allowed to under the seconding Member State's national law. The host Member State may prohibit the carrying of particular arms, ammunition or equipment			
Mechanisms to ensure Data Protection when accessing/exchanging information	Each Member State shall guarantee a level of protection of personal data in its national law at least equal to that resulting from the Council of Europe Convention for the Protection of Individuals and its Additional Protocol			
Requirement to develop cross-border threat assessment/risks analysis				

Source: Author's own elaboration

Non-binding

Table 11 – Overview of non-binding EU measures with respect to operational cooperation for SOC and terrorism

	Council Document 10000/07 (European Union Manual: Traces on the Ownership of Firearms)	Council Document 15785/3/10 (Schengen Catalogue of Recommendations and Best practices: Police cooperation)	Council Document 13887/20 (Manual on cross-border operations)	Council document 15429/16 (Handbook for the Naples II Convention)	Council Document 10590/18 (Guidance on the Naples II Convention)
Objective		Catalogue of recommendations and best practices for customs authorities engaged in cross-border cooperation. Customs shall provide each other with the necessary assistance in terms of staff and organisational support	Manual helping set up joint investigation teams		
Relevant crime area		Traffic of drugs and psychotropic substances, weapons, munitions, explosive materials, cultural goods, dangerous and toxic waste, nuclear material or materials or equipment intended for the manufacture of atomic, biological and/or chemical weapons (prohibited goods); Trade in narcotic drugs and psychotropic substances and intended for the illegal manufacture of drugs (precursor substances); Trade in taxable goods to evade tax or to obtain unauthorised State payments in connection with the import or export of goods, trade in goods prohibited	Cross-border crimes (including terrorism)		
Type of law enforcement cooperation activity concerned		Joint operations	Intelligence/information sharing, joint operations		
Main features of the cooperation activity		If necessary, the participating authorities shall apply to their judicial authorities for approval of the planned investigations. Information obtained by officers	Member States can cooperate: To request investigative measures between team members directly, dispensing with the need for Letters Rogatory (this applies also to		

	Council Document 10000/07 (European Union Manual: Traces on the Ownership of Firearms)	Council Document 15785/3/10 (Schengen Catalogue of Recommendations and Best practices: Police cooperation)	Council Document 13887/20 (Manual on cross-border operations)	Council document 15429/16 (Handbook for the Naples II Convention)	Council Document 10590/18 (Guidance on the Naples II Convention)
		during cross-border cooperation may be used, in accordance with national law and subject to particular conditions laid down by the competent authorities of the State in which the information was obtained, as evidence by the competent bodies of the Member State receiving the information. Requests for assistance shall always be made in writing.	requests for coercive measures, be present at house searches, interviews, etc. in all jurisdictions covered, helping overcome language barriers in interviews etc.); To Co-ordinate efforts on the spot, and for informal exchange of specialised knowledge; To build mutual trust between practitioners from different jurisdictions working together and deciding on investigative and prosecution strategies, With Europol and Eurojust for direct support and assistance, secure potentially available funding		
Stakeholders involved		Customs authorities	Police, LEAs		
Criteria for developing joint operations					
Specific requirements for the use of arms/equipment			Depending on national legislation		
Mechanisms to ensure Data Protection when accessing/exchanging information					
Requirement to develop cross-border threat assessment/risks analysis					

Source: Author’s own elaboration

Measures focused on specific investigative tools

2.4.1.1 Controlled deliveries

Table 12 – Overview of EU measures focused on specific investigative tools - Controlled deliveries

	Binding			Non-binding	
	Convention implementing the Schengen Agreement (CISA)	Naples II Convention	Council Document 13887/20 (Manual on cross-border operations)	Council document 15429/16 (Handbook for the Naples II Convention)	Council Document 10590/18 (Guidance on the Naples II Convention)
How is the tool defined?	The measure has the objective to allow controlled deliveries to be made in the context of the illicit trafficking in narcotic drugs and psychotropic substances	Special form of cooperation	A controlled delivery is a technique of allowing illicit or suspect consignments of substances or objects or substitutions for these to pass out of, through or into the territory of one or more countries, with the knowledge and under the supervision of the competent authorities, with a view to establishing who is criminally involved	The document's aim is to provide a common framework of the contact details of all the Member States authorities involved in controlled deliveries activities within a Member State	Controlled delivery is a working method in which suspicious or illicit consignments of goods are not seized at the frontier but are kept under surveillance until they reach their final destination
For what types of SOC can the tool be used?	Illicit trafficking in narcotic drugs and psychotropic substances	Controlled deliveries may be permitted in the framework of criminal investigations into extraditable offences	Control of drug and other goods		Infringement included in the Naples II Convention

	Binding			Non-binding	
	Convention implementing the Schengen Agreement (CISA)	Naples II Convention	Council Document 13887/20 (Manual on cross-border operations)	Council document 15429/16 (Handbook for the Naples II Convention)	Council Document 10590/18 (Guidance on the Naples II Convention)
What types of stakeholder are involved in the implementation of this tool?		Member States competent authority and customs authorities			Competent authorities of Member States
Which LEAs can use this tool?		Customs authorities			
What are the rules to be followed for the implementation of this tool?		Requests for cooperation shall take the form of requests for assistance. Member States shall appoint in their customs authorities a central unit (coordinating unit) responsible for receiving all applications for mutual assistance under Naples II Convention and for coordinating mutual assistance. The coordinating units of the Member States shall maintain the necessary direct contact with each other	A controlled delivery can be carried out if permission was granted in advance. Where the controlled deliveries involve more than two Member States, authorisation must be obtained from the transit and destination Member State(s). The special conditions and approval procedures for authorising a controlled delivery differ between Member States		Prepare and complete the forms requesting a controlled delivery; Establish contact with the central coordinating units most likely to be involved in a case of a controlled delivery; Establish contact with national authorities responsible for taking the decision to allow a controlled delivery; Make a contact list of all the operational units involved, clarify and resolve any queries or uncertainties that may arise; Practice a controlled delivery with your own organisation and neighbouring Member States; Appoint centralised units and/or specialised officers for the coordination of operations; Prepare a national practical manual for controlled deliveries, as a supplement to the national fact sheets in the handbook
What authorisation is needed for the use of this tool?		The decision to carry out controlled deliveries shall be taken in each individual case by the competent authorities of the requested Member State, with due regard for the national law of that State			The competent authority and/or the central coordinating unit should be contacted early in the planning of a controlled deliver
What thresholds must be passed for the use of this tool?					Urgent case (depending on the specific situation)
What ongoing supervision is required for the use of this tool?			The host state shall be responsible for leading and monitoring the operation on its territory and shall have the authorisation to intervene		

Source: Author's own elaboration

2.4.1.2 Hot pursuit

Table 13 – Overview of EU measures focused on specific investigative tools – Hot pursuit

	Binding			Non-binding	
	Convention implementing the Schengen Agreement (CISA)	Naples II Convention	Council Document 13887/20 (Manual on cross-border operations)	Council document 15429/16 (Handbook for the Naples II Convention)	Council Document 10590/18 (Guidance on the Naples II Convention)
How is the tool defined?	Officers of one of the Contracting Parties who are pursuing in their country an individual caught in the act of committing or of participating in one of the offences listed in the CISA	Special form of cooperation	A cross-border pursuit is the continued pursuit of subjects suspected of or caught when committing a specific crime type crossing a national border into another Member State (State B)	The document's aim is to provide a common framework of the contact details of all the MS authorities involved in hot pursuit activities within a MS.	This article allows customs officers as well as officers from other competent authorities to continue the pursuit of an individual on the territory of another Member State, whether on land, in the air or at sea. This pursuit can be carried out without prior authorisation.
For what types of SOC can the tool be used?	Murder, manslaughter, rape, arson, forgery of money, aggravated burglary and robbery and receiving stolen goods, extortion, kidnapping and hostage taking, trafficking in human beings, illicit trafficking in narcotic drugs and psychotropic substances, breach of the laws on arms and explosives, wilful damage through the use of explosives, illicit transportation of toxic and hazardous waste, failure to stop and give particulars after an accident which has resulted in death or serious injury	Extraditable offences	Each State has the choice between two options for the types of offence allowing the power of pursuit to be exercised (list of offences listed in Article 41(4)(a) CISA or extraditable offences)		Infringement referred to in Article 19(2) in Naples II Convention
What types of stakeholder are involved in the implementation of this tool?	Police and customs authorities	Customs authorities			Judicial Police Authorities of MS
Which LEAs can use this tool?	Police and customs authorities	Customs authorities			Judicial Police Authorities of MS
What are the rules to be followed for the implementation of this tool?	Officers who are pursuing in their country an individual caught in the act of committing or of participating in one of the offences shall be authorised to continue pursuit in the territory of another Contracting Party without the latter's prior authorisation where, given the particular urgency of the situation, it is not possible to notify the competent authorities of the other Contracting Party prior to entry into that territory. The same shall apply where the person being pursued has escaped from provisional custody or while serving a sentence involving deprivation of liberty	The pursuing officers shall, not later than when they cross the border, contact the competent authorities of the Member State in whose territory the pursuit is to take place. The pursuit shall cease as soon as the Member State in whose territory the pursuit is taking place so requests. At the request of the pursuing officers, the competent authorities of the said Member State challenge the pursued person so as to establish his identity or to arrest him. Member States shall inform the depositary of the pursuing officers and the depositary shall inform the other Member States. The pursuing officers do not have the right to apprehend. If no request to cease the pursuit is made and if the competent authorities of the Member State in whose territory the pursuit is taking place are unable to intervene quickly enough, the pursuing officers may apprehend the person pursued until the officers of the said Member State, who must be informed without delay, are able to establish his identity or arrest him.	The person concerned must have been caught in the act of committing or participating in one of the offences and/or the person concerned is under provisional arrest or serving a custodial sentence. Hot pursuit requires that: - It has not been possible to advise the requested authorities in advance owing to particular urgency; - The authorities have been advised but have not been able to take up the pursuit in good time themselves; - The pursuing officers consult the authorities of the requested State at the latest upon crossing the border; - The pursuit cease at the first request of the requested State. Pursuit may be restricted: territorially, timely or there may be a restriction on the powers of the pursuing agents. It is mandatory to inform the authorities of the State on the territory of which the pursuit is being carried out at the latest upon		Infringement included in the Naples II Convention that could give rise to extradition

	Binding			Non-binding	
	Convention implementing the Schengen Agreement (CISA)	Naples II Convention	Council Document 13887/20 (Manual on cross-border operations)	Council document 15429/16 (Handbook for the Naples II Convention)	Council Document 10590/18 (Guidance on the Naples II Convention)
		The pursuing officers comply with the law of the Member State in whose territory they are operating. They shall obey the instructions of the competent authorities of the said Member State. When the pursuit takes place on the sea, it shall, where it extends to the high sea or the exclusive economic zone, be carried out in conformity with the international law of the sea as reflected in the United Nations Convention on the Law of the Sea, and, when it takes place in the territory of another Member State, it shall be carried out in accordance with the provisions of this Article; entry into private homes and places not accessible to the public shall be prohibited. The pursuing officers shall be easily identifiable, either by their uniform or an armband or by means of accessories fitted to their means of transport; the use of civilian clothes combined with the use of unmarked means of transport without the aforementioned identification is prohibited. The pursuing officers shall at all times be able to prove that they are acting in an official capacity	crossing the border (State B). This must be done by contacting either the first police authority of the State concerned or one of the liaison authorities designated by the State concerned. The officers must act in compliance with the national law of the state in which they are operating and must follow the instructions of the locally competent authorities. The pursuit must be stopped at the request of the authorities of State B. The officers must be in possession of their service badge or pass and be easily identifiable (uniform, armband, vehicle, etc.). The officers may carry his service weapon and its use is forbidden apart from in self-defence under the national law of State B. The arrested person should be given into the custody of the locally competent authorities. If the person is arrested, the person may be held for questioning by the competent local authorities whatever his nationality. If the person is arrested and is not a national of the country where the arrest was made, the person must be released six hours after arrest if no provisional arrest warrant for extradition is forthcoming. The persons arrested may only be subjected to a security search for the purpose of bringing them before the local authorities. They may be hand-cuffed and objects on their person may be seized. The officers involved must appear before the locally competent authorities to make a report after every pursuit, no matter what the outcome; if the latter so wish, the officers must remain available and provide assistance, if requested, with the follow-up, investigations and judicial procedures.		
What authorisation is needed for the use of this tool?	Just to inform the authority of the other Contracting Party		It is mandatory to inform the competent authorities of the Member State in whose territory the pursuit is to take place		Communication to the neighbouring country
What thresholds must be passed for the use of this tool?					The urgency of the situation makes it impossible for prior notification to be given
What ongoing supervision is required for the use of this tool?		Member States competent authority	The officers must act in compliance with the national law of the state in which they are operating and must follow the instructions of the locally competent authorities		To inform the competent authorities of the other Member States at the latest when crossing the border

Source: Author's own elaboration

2.4.1.3 Surveillance

Table 14 – Overview of EU measures focused on specific investigative tools - Surveillance

	Binding	Non-binding
	Naples II Convention	Council Document 13887/20 (Manual on cross-border operations)
How is the tool defined?	Special form of cooperation	A cross-border surveillance is an operation whereby a surveillance operation in one State (A - "requesting State") is continued onto the territory of another State (B - "requested State"). This can be done either by the officers having started the surveillance or it can be a continuation by officers of State B. The surveillance can cross several States.
For what types of SOC can the tool be used?	Traffic of drugs and psychotropic substances, weapons, munitions, explosive materials, cultural goods, dangerous and toxic waste, nuclear material or materials or equipment intended for the manufacture of atomic, biological and/or chemical weapons (prohibited goods); trade in narcotic drugs and psychotropic substances and intended for the illegal manufacture of drugs (precursor substances); trade in taxable goods to evade tax or to obtain unauthorised State payments in connection with the import or export of goods, trade in goods prohibited	Pre-planned surveillance: offences punishable under the laws of the requesting Party and of the requested Party by deprivation of liberty or under a detention order for a maximum period of at least one year or by a more severe penalty; Urgent surveillance: having committed one of the offences mentioned in Article 40(7), as amended by Council Decision 2003/725/JHA Designated national competent authority
What types of stakeholder are involved in the implementation of this tool?		
Which LEAs can use this tool?	Customs authorities	
What are the rules to be followed for the implementation of this tool?	Request for assistance shall be presented before the surveillance and to be sent to an authority designated by each of the Member States empowered to grant the requested authorisation or pass on the request. Member States shall inform the depositary of the officers to whom this provision applies. If for urgent reasons the authorisation cannot be requested, the competent authorities of the Member State in whose territory the observation is to be continued is to be notified immediately of the crossing of the border, during the observation and a request of authorisation outlining the grounds for crossing the border without prior authorisation shall be submitted. The officers conducting the observation comply with the law of the Member State in whose territory they are operating; they must obey the instructions of the competent authorities of the said Member State without delay. The officers carry a document certifying that authorisation has been granted. The officers shall be able to provide proof that they are acting in an official capacity. They may carry their service weapons during the observation save where the requested Member State has made a general declaration that weapons may never be carried into its territory or where specifically decided otherwise by the requested Member State. When officers are permitted to carry their service weapons, their use shall be prohibited save in cases of legitimate self-defence. Officers cannot entry into private homes and places not accessible to the public. Officers conducting the observation may neither challenge nor arrest the person under observation and all operations shall be the subject of a report to the authorities of the Member State in whose territory they took place.	Urgent surveillance: There are "particularly urgent reasons" that made it impossible to request prior authorisation. The designated authority of state B is immediately notified that the border has been crossed. A request for assistance is submitted without delay to the designated authority using the standard form. In urgent cases a request can be received from the foreign authority on the telephone, but in that case the information shall be confirmed in writing as soon as possible. An urgent reply is necessary from State B as to whether the request is approved or rejected. If state B remains silent, the urgent surveillance must stop 5 hours from the time of crossing the border. The officers must contact the nearest authority responsible for police tasks when they cross the border or a national contact point, depending on national structures. The surveillance must cease either at the request of state B or if no approval has been obtained from state B within 5 hours after the border was crossed. Pre-planned surveillance: A request for assistance is first submitted via the designated (central) authorities of each state, using the standard form. State B can decide to grant the authorisation for a specific period of time (e.g. from a couple of days to a couple of months). Authorities must be notified before the start of the surveillance. The officers carrying out the surveillance must carry a document certifying the authorisation to carry out the surveillance. 24/7 Requests: The competent authorities in State B must be able to consider a request on a 24/7 basis. In some Member States the carrying out of a cross-border surveillance necessitates a request for judicial assistance. Some Member States require an additional request for judicial assistance, for example a European investigation order. State B can authorise the surveillance as requested, can attach conditions or can refuse the request. State B replies on the same form as the one which was sent to it. The authorisation should clearly state the law enforcement agency in state B that will support the surveillance. Only officers from designated authorities are authorised to perform cross-border surveillance. The officers are subject to and must comply with the national law of the country in which they are operating (State B). The officers must follow the instructions of the locally competent authorities. The officers carrying out the surveillance must at all times be able to give proof of their acting in an official capacity. Unless state B expressly objects, the officers may carry their service weapons; their use is prohibited except in cases of legitimate self-defence under the national law of the requested country. Entry into homes and places not accessible to the public is prohibited. The officers carrying out the surveillance may neither challenge nor arrest the person under surveillance. This does not prevent in exceptional

	Binding	Non-binding
	Naples II Convention	Council Document 13887/20 (Manual on cross-border operations)
		circumstances the officers’ ability to intervene to prevent or stop a crime, as any citizen should do.
What authorisation is needed for the use of this tool?	Request for assistance to be presented before the surveillance and to be sent to an authority designated by each of the Member States empowered to grant the requested authorisation or pass on the request	Urgent surveillance: There are "particularly urgent reasons" that made it impossible to request prior authorisation. The designated authority of State B is immediately notified that the border has been crossed. A request for assistance is submitted without delay to the designated authority using the standard form. In urgent cases a request can be received from the foreign authority on the telephone, but in that case the information shall be confirmed in writing as soon as possible. An urgent reply is necessary from state B as to whether the request is approved or rejected. Planned surveillance: A request for assistance is first submitted via the designated (central) authorities of each state, using the standard form. The competent authorities in state B must be able to consider a request on a 24/7 basis. In some Member States the carrying out of a cross-border surveillance necessitates a request for judicial assistance. Some Member States therefore require an additional request for judicial assistance, for example a European investigation order. State B can authorise the surveillance as requested, can attach conditions or can refuse the request. State B replies on the same form as the one which was sent to it
What thresholds must be passed for the use of this tool?	Serious grounds for believing that the one observed is involved in: Traffic of drugs and psychotropic substances, weapons, munitions, explosive materials, cultural goods, dangerous and toxic waste, nuclear material or materials or equipment intended for the manufacture of atomic, biological and/or chemical weapons (prohibited goods); Trade in narcotic drugs and psychotropic substances and intended for the illegal manufacture of drugs (precursor substances); Trade in taxable goods to evade tax or to obtain unauthorised State payments in connection with the import or export of goods, trade in goods prohibited	
What ongoing supervision is required for the use of this tool?	Member States competent authority	The officers are subject to and must comply with the national law of the country in which they are operating (State B). The officers must follow the instructions of the locally competent authorities, i.e. the authorities in the district where the surveillance takes place.

Source: Author’s own elaboration

2.4.1.4 Covert investigations

Table 15 – Overview of EU measures focused on specific investigative tools – Covert investigations

	Binding	Non-binding
	Naples II Convention	Council document 15429/16 (Handbook for the Naples II Convention)
How is the tool defined?	Special form of cooperation	The document's aim is to provide a common framework of the contact details of all the Member States authorities involved in covert investigation activities within a Member State
For what types of SOC can the tool be used?		
What types of stakeholder are involved in the implementation of this tool?	Customs authorities	
Which LEAs can use this tool?	Customs authorities	
What are the rules to be followed for the implementation of this tool?	The covert investigation shall be authorised by the requested Member States and shall have a limited duration. The preparation and supervision of the investigations shall take place in close cooperation between the relevant Member States authorities. The conditions under which a covert investigation is allowed and carried out shall be determined by the requested authority in accordance with its national law. The requested authority shall provide the necessary manpower and technical support	
What authorisation is needed for the use of this tool?	Authorisation from the competent authority of the requested Member States	

	Binding	Non-binding
	Naples II Convention	Council document 15429/16 (Handbook for the Naples II Convention)
What thresholds must be passed for the use of this tool?		
What ongoing supervision is required for the use of this tool?	Competent authority of the requested Member States	

Source: Author’s own elaboration

2.5 Data protection

Table 16 – Overview of EU measures with respect to data protection⁷

	Directive 2002/58/EC (Processing of personal data and the protection of privacy in the electronic communications sector)	Regulation 2016/679 (GDPR)	Directive (EU) 2016/680 (Law enforcement directive)	Regulation 2018/1725 (Processing of personal data by the Union institutions, bodies, offices and agencies)
Objective	To set out rules to ensure security in the processing of personal data, the notification of personal data breaches, and confidentiality of communications as well to ban unsolicited communications where the user has not given their consent	To allow EU citizens to better control their personal data as well as to modernise and unify rules allowing businesses to reduce red tape and to benefit from greater consumer trust	To better protect individuals’ personal data when their data are being processed by police and criminal justice authorities; to improve cooperation in the fight against terrorism and cross-border crime in the EU by enabling police and criminal justice authorities in EU countries to exchange information necessary for investigations more efficiently and effectively.	To lay down rules on how EU institutions, bodies, offices and agencies should treat the personal data they hold on individuals; to uphold individuals’ fundamental rights and freedoms, especially the right to protection of personal data and the right to privacy; to align the rules for EU institutions, bodies, offices and agencies with those of the general data protection regulation (GDPR) and of Directive (EU) 2016/680
Type of information to be exchanged	Personal data, in particular traffic data; location data any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service	Personal data	Personal data	Personal data
Tools/ information systems used to exchange information				
Specific actors involved in the exchange of information	Police or national competent authority	Everyone	Competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security	Union institution and body
Timing for exchanging information				
Language to be used for the exchange of information				
Requirements for exchanging information relating to specific areas				
Mechanisms to ensure Data Protection when accessing/exchanging information	Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of	Personal data shall be: Processed lawfully, fairly and in a transparent manner in relation to the data subject; Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;	Personal data shall be: Processed lawfully, fairly and in a transparent manner in relation to the data subject; Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;	Personal data shall be: Processed lawfully, fairly and in a transparent manner in relation to the data subject; Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

⁷ More EU measures provide for data protection rules in specific situation (e.g. Decisions 2007/533/JHA and Regulation (EU) 2018/1862). The ones in the table represent the most relevant and meaningful. Decisions 2007/533/JHA and Regulation (EU) 2018/1862 are on the establishment, operation and use of the first and second generation of the Schengen Information System. Among the rules they also provide for data protection indications but referring to other legislative measures or other instruments (e.g. as art. 57 Regulation (EU) 2018/1862 “Personal data processed in application of this Decision shall be protected in accordance with the Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data, and subsequent amendments thereto”; art 58 “The right of persons to have access to data relating to them entered in SIS II in accordance with this Decision shall be exercised in accordance with the law of the Member State before which they invoke that right”. In my opinion the legislative measures analysed in the table provide for factual, practical and operative rules and can be representative of the whole legal measures on data protection.

	Directive 2002/58/EC (Processing of personal data and the protection of privacy in the electronic communications sector)	Regulation 2016/679 (GDPR)	Directive (EU) 2016/680 (Law enforcement directive)	Regulation 2018/1725 (Processing of personal data by the Union institutions, bodies, offices and agencies)
	communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so	Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures	Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures	Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures
Requirement to develop cross-border threat assessment/risks analysis				

Source: Author's own elaboration

2.6 EU Agencies' legal basis

Table 17 – Overview of the legal basis of EU Agencies

	Regulation 1920/2006 (EMCDDA)	Regulation (EU) 2015/2219 (CEPOL)	Regulation 2016/794 (Europol)	Regulation 2018/1726 (eu-LISA)	Regulation 2018/1727 (Eurojust)	Regulation 2019/1896 (EBCGA/Frontex)
Objective	To provide a common framework on the drug use and addiction by sharing relevant information between MSs by setting up the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA). The Centre shall have at its disposal the European Information Network on Drugs and Drug Addiction (Reitox)	The measure relates to the enforcement of a special training programme for senior police officers. Regulation only provides that national units, established or designated by MSs, shall supply to CEPOL information necessary for carry out its tasks.	Europol shall support and strengthen action by the competent authorities of the Member States even by sharing information	eu-LISA shall ensure: • <u>The development of large-scale IT systems using an adequate project management structure;</u> • <u>The effective, secure and continuous operation of large-scale IT systems;</u> • <u>The efficient and financially accountable management of large-scale IT systems;</u> • <u>An adequately high quality of service for users of large-scale IT systems;</u> • <u>Continuity and uninterrupted service;</u> • <u>A high level of data protection, in accordance with EU data protection law, including specific conditions for each large-scale IT system;</u> • <u>An appropriate level of data and physical security;</u>	Eurojust shall support and strengthen coordination and cooperation between national investigating and prosecuting authorities in relation to serious crime which Eurojust is competent to deal with where that crime affects two or more Member States, or requires prosecution on common bases	This Regulation establishes EUROSUR as an integrated framework for the exchange of information and for operational cooperation within the European Border and Coast Guard (FRONTEX) in order to improve situational awareness and to increase reaction capability for the purposes of border management, including the detection, prevention and combating of illegal immigration and cross-border crime and contributing to ensuring the protection and saving the lives of migrants

	Regulation 1920/2006 (EMCDDA)	Regulation (EU) 2015/2219 (CEPOL)	Regulation 2016/794 (Europol)	Regulation 2018/1726 (eu-LISA)	Regulation 2018/1727 (Eurojust)	Regulation 2019/1896 (EBCGA/Frontex)
Type of information to be exchanged	Collecting, registering and analysing information, including data resulting from research, communicated by Member States and data emanating from Community, non-governmental national sources and competent international organisations, including the European Police Office (Europol); Providing information on best practices in the Member States and facilitating the exchange of such practices among them. Collection, registration, analysis and information work shall also cover data on emerging trends in poly-drug use, including the combined use of licit and illicit psychoactive substances		Personal data, confidential documents, intelligence and financial records, information on international events	including specific rules for each large-scale IT system.	Personal data, cases already stored by Eurojust, cases in which conflicts of jurisdiction have arisen or are likely to arise, controlled deliveries affecting at least three countries, at least two of which are Member States, repeated difficulties or refusals regarding the execution of requests for, or decisions on, judicial cooperation, including requests and decisions based on instruments giving effect to the principle of mutual recognition	Information related to the performance of Agency's tasks
Tools/ information systems used to exchange information	Reitox					The Agency shall establish and maintain a communication network in order to provide communication and analytical tools and allow for the exchange of sensitive non-classified and classified information in a secure manner. Each Member State shall appoint a national contact point for communication with the Agency on all matters pertaining to the activities of the Agency
Specific actors involved in the exchange of information	EMCDDA and Reitox	National units of MS shall each year supply CEPOL with the information necessary for it to carry out its tasks; Each year the Executive Director shall send all information relevant to the findings of any evaluation procedures to the European Parliament and to the Council and shall also notify the Court of Auditors of any such findings.	Europol shall only process information that has been provided to it by: Member States; Union bodies, third countries and international organisations; Private parties, partners and private persons Liaison officers shall assist in the exchange of information between Europol and OLAF (European Anti-Fraud Office)		The competent authorities of the Member States shall exchange with Eurojust all information necessary for the performance of its tasks. In operational matters relevant to the European Public Prosecutor's Office (EPPO) competences, Eurojust shall inform the EPPO of and, where appropriate, associate it with its activities concerning cross-border cases	FRONTEX and Member States shall exchange information as listed in the boxes above
Timing for exchanging information						
Language to be used for the exchange of information						
Requirements for exchanging information relating to specific areas			Europol shall establish rules on the protection of EU classified information			
Mechanisms to ensure Data Protection when	Personal data are not collected	CEPOL should promote common respect for, and	If Europol receives information, including personal data, from a private person residing in a	The processing of personal data by the Agency shall be subject to Regulation (EU) 2018/1725.	The Regulation only states that Eurojust and Member States shall define mechanisms to	

	Regulation 1920/2006 (EMCDDA)	Regulation (EU) 2015/2219 (CEPOL)	Regulation 2016/794 (Europol)	Regulation 2018/1726 (eu-LISA)	Regulation 2018/1727 (Eurojust)	Regulation 2019/1896 (EBCGA/Frontex)
accessing/exchanging information		understanding of data protection.	third country with which there is no international agreement concluded, Europol may only forward that information to a Member State or to a third country concerned with which such an international agreement has been concluded	Measures pursuant such Regulation shall be adopted after consulting the European Data Protection Supervisor. The Agency may process personal data only: • <u>Where necessary for the performance of its tasks related to the operational management of large-scale IT systems entrusted to it under Union law;</u> • <u>Where necessary for its administrative tasks.</u>	ensure that the security measures are addressed across information system boundaries	
Requirement to develop cross-border threat assessment/risks analysis	Collecting, registering and analysing information, including data resulting from research, communicated by Member States and data emanating from Community, non-governmental national sources and competent international organisations, including the European Police Office (Europol); Providing information on best practices in the Member States and facilitating the exchange of such practices among them. Collection, registration, analysis and information work shall also cover data on emerging trends in poly-drug use, including the combined use of licit and illicit psychoactive substances		A report including statistical information regarding complaints, inquiries, and investigations must be performed without any further specification. Actors in charge of performing cross-border threat assessment/risks analysis are Europol and EDPS (European Data Protection Supervisor)			The Agency shall monitor migratory flows towards the EU, and within the EU in terms of migratory trends, volume and routes, and other trends or possible challenges at the external borders and with regard to return. The Agency shall prepare general annual risk analyses, which shall be submitted to the European Parliament, to the Council and to the Commission. Every two years, the Agency, in close consultation with the Member States, shall prepare and submit to the European Parliament, to the Council and to the Commission a strategic risk analysis for European integrated border management. Such strategic risk analyses shall be taken into account for the preparation of the multiannual strategic policy cycle for European integrated border management. The Agency shall prepare such general annual risk analyses and strategic risk analyses on the basis of information received, including from the Member States. Personal data shall be anonymised in the results of such risk analyses

Source: Author's own elaboration

3 NATIONAL RULES ON INVESTIGATIVE TOOLS USED TO FIGHT SERIOUS AND ORGANISED CRIME

Austria

Table 18 – Overview of national rules on investigative tools - Austria

Relevant items	Provisions	Sources used
Controlled Delivery		
Relevant documents (legal and non-legal) that define the functioning of the tool	- Law on Judicial Cooperation in Criminal Matters with the Member States of the European Union (Bundesgesetz über die justizielle Zusammenarbeit in Strafsachen mit den Mitgliedstaaten der Europäischen Union (EU-JZG)). - Law on extradition and mutual legal assistance in criminal matters (Auslieferungs- und Rechtshilfegesetz (ARHG)). - Controlled delivery in cross-border settings is also regulated in bilateral agreements with the bordering countries. Since the agreements with bordering countries mainly specify the ground rules set in the EU-JZG, the EU-JZG shall suffice as a reference here for consistency reasons.	- EU-JZG: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20003339 - ARHG: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002441
How is the tool defined?	Controlled delivery is the transport of objects from, into or through the Federal territory, insofar as the prosecution would be entitled to proceed under section 99 para. 4 of the Code of Criminal Procedure (CCP).	Section 71 EU-JZG.
For what types of crime can the tool be used?	Cross crime areas. The relevant clauses, sections 71 and 72 EU-JZG do not specify certain types of crimes the tool can be used for. However, there is a limit in the use of the tool imposed by section 72 para. 3 EU-JZG, according to which a controlled delivery is prohibited if the special nature of the goods or of the group of offenders could cause a serious danger to the life, health, physical integrity or freedom of a person. Furthermore, section 71 EU-JZG refers to 99 para. 4 CCP, which states that the postponement of investigative action must not take place if this poses a serious risk to the life, health, physical integrity or freedom of third parties. One area where this prohibition surely applies is trafficking of human beings.	- Section 71 EU-JZG. - Section 72 EU-JZG. - Section 99 para. 4 CCP. - Criminal Code https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002326
Does national law allow this tool to be used in cross-border cases?	The tool is specifically designed for cross-border cases.	- Section 71 EU-JZG. - Section 72 EU-JZG.
What thresholds must be passed for the use of this tool?	Since the use of the tool is not limited to certain types of crimes, there is no specific answer on the maximum imprisonment term for respective crimes. In general, the maximum term of imprisonment in Austria is lifetime imprisonment. Most crimes threatened with lifetime sentences are listed in the Austrian Criminal Code (CC) and are mostly related to causing the death of other people. Moreover, section 28a para. 5 of the Austrian Addictive Drug Act (Suchtmittelgesetz / SMG) sets a possible lifetime sentence if the offender has a leading position in an organisation conducting organised drug trafficking.	- Section 71 EU-JZG. - Section 72 EU-JZG. - Criminal Code https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002326 - Section 28a para. 5 SMG https://www.ris.bka.gv.at/GeltendeFassung/Bundesnormen/10011040/SMG%2c%20Fassung%20vom%2008.03.2021.pdf
What types of stakeholder are involved in the implementation of this tool?	LEAs.	Section 72 EU-JZG.
Which LEAs can use this tool?	The criminal police is the initiating and executing body. The use of the tool can also be initiated by foreign authorities. The prosecution is the authorising body.	Section 72 para. 1 EU-JZG.
What are the rules to be followed for the implementation of this tool?	- A controlled delivery can be made either on request or in agreement with another member state. The criminal police is the initiating body. The criminal police shall immediately notify the public prosecutor's office of a planned controlled delivery. - After notification, the public prosecution has to decide on the approval of the controlled delivery. The prosecution office responsible is the one, in whose territory the border is likely to be crossed or from whose territory the controlled delivery is to originate. If such an office cannot be determined, the prosecution office Vienna is responsible.	Section 72 EU-JZG.
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	There is a limit in the use of the tool imposed by section 72 para. 3 EU-JZG, according to which a controlled delivery is prohibited if the special nature of the goods or of the group of offenders could cause a serious danger to the life, health, physical integrity or freedom of a person. Furthermore, section 71 EU-JZG refers to 99 para. 4 CCP, which states that the postponement of investigative action must not take place if this poses a serious risk to the life, health, physical integrity or freedom of third parties. One area where this prohibition surely applies is trafficking of human beings.	- Section 71 EU-JZG. - Section 72 EU-JZG. - Section 99 para. 4 CCP. https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002326
What authorisation is needed for the use of this tool?	Authorisation by the prosecution is needed before criminal police can use the tool.	Section 72 para. 1 EU-JZG.
What ongoing supervision is required for the use of this tool?	There is no defined supervisory unit to observe the controlled delivery. However, it must always be designed in such a way that access to the suspects and the goods is possible at any time.	Section 72 para. 4 EU-JZG.
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	

Relevant items	Provisions	Sources used
Data available on the number of times this tool has been used for SOC cases	N/A	
Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	There is no specific national law on hot pursuit in Austria. Since the Convention implementing the Schengen Agreement (Schengen Convention) applies to Austria, Art. 41 Schengen Convention is the basic relevant law. Additionally, bilateral (for Liechtenstein and Switzerland multilateral) agreements exist for interstate police cooperation with all countries bordering Austria, all of them containing rules on hot pursuit. Those rules are mainly specifying Art. 41 Schengen Convention. All of the agreements are subject to cross-border police cooperation. The agreement partners in specific are: - Germany - Italy - Switzerland - Liechtenstein - Slovakia - Slovenia - Hungary - Czechia	- Schengen Convention: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A42000A0922%2802%29 - Agreement with Germany: https://www.ris.bka.gv.at/Ergebnis.wxe?Abfrage=BgblAuth&Bgblnummer=210/2005&SucheNachTeil3=True - Agreement with Italy: https://www.ris.bka.gv.at/Ergebnis.wxe?Abfrage=BgblAuth&Bgblnummer=47/2017&SucheNachTeil3=True - Agreement with Switzerland and Liechtenstein: https://www.ris.bka.gv.at/Ergebnis.wxe?Abfrage=BgblAuth&Bgblnummer=78/2017&SucheNachTeil3=True - Agreement with Switzerland: https://www.ris.bka.gv.at/Ergebnis.wxe?Abfrage=BgblAuth&Bgblnummer=78/2017&SucheNachTeil3=True - Agreement with Slovakia: https://www.ris.bka.gv.at/Ergebnis.wxe?Abfrage=BgblAuth&Bgblnummer=72/2005&SucheNachTeil3=True - Agreement with Slovenia: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20004037 - Agreement with Hungary: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20004823 - Agreement with Czechia: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20004858
How is the tool defined?	Since the agreements with bordering countries mainly specify the ground rules set in the Schengen Convention, the Schengen Convention shall suffice as a reference here for consistency reasons.	Art 41 para. 1 Schengen Convention
For what types of crime can the tool be used?	The following crime types are listed in Art 41 Schengen Convention: murder, manslaughter, rape, arson, forgery of money, aggravated burglary and robbery and receiving stolen goods, extortion, kidnapping and hostage taking, trafficking in human beings, illicit trafficking in narcotic drugs and psychotropic substances, breach of the laws on arms and explosives, wilful damage through the use of explosives, illicit transportation of toxic and hazardous waste, failure to stop and give particulars after an accident which has resulted in death or serious injury. - Germany: Types listed in Art 41 Schengen Convention. Additions made in the agreement: Up to 150 km after the border hot pursuit is allowed for the purpose of tracing persons suspected of committing an extraditable criminal offence or sentenced to a custodial sentence. - Italy: Art 41 Schengen Convention fully applies. Furthermore, hot pursuit is allowed if a person is suspected of participating in or committing an offence which falls within the scope of the of the European arrest warrant. - Slovakia: Similar phrasing as the Schengen Convention. - Liechtenstein: Similar phrasing as the Schengen Convention. - Switzerland: Similar phrasing as the Schengen Convention. - Slovenia: Similar phrasing as the Schengen Convention. - Hungary: Similar phrasing as the Schengen Convention. Furthermore, hot pursuit is allowed if a person is suspected of participating in or committing an offence which falls within the scope of the of the European arrest warrant. - Czechia: Similar phrasing as the Schengen Convention. Furthermore, hot pursuit is allowed if a person is suspected of participating in or committing an offence which falls within the scope of the of the European arrest warrant.	- Art 41 para 1. and para. 4 Schengen Convention. - Germany: Art 12 in the respective agreement. - Italy: Art 12 in the respective agreement. - Slovakia: Art 8 in the respective agreement. - Switzerland: Art 15 in the respective agreement. - Slovenia: Art 9 in the respective agreement. - Hungary: Art 11 and Art 12 in the respective agreement. - Czechia: Art 11 in the respective agreement.
Does national law allow this tool to be used in cross-border cases?	The tool is specifically designed for cross-border cases.	- Art 41 para 1. and para. 4 Schengen Convention. - Germany: Art 12 in the respective agreement. - Italy: Art 12 in the respective agreement. - Slovakia: Art 8 in the respective agreement. - Switzerland: Art 15 in the respective agreement. - Slovenia: Art 9 in the respective agreement. - Hungary: Art 11 and Art 12 in the respective agreement. - Czechia: Art 11 in the respective agreement.

Relevant items	Provisions	Sources used
What thresholds must be passed for the use of this tool?	The tool can be used for various types of crimes. The sentences for these range up to life in prison. The sentences for these crimes range up to life imprisonment (e.g. murder).	Criminal Code: https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296
What types of stakeholder are involved in the implementation of this tool?	LEAs.	- Germany: Art 12 in the respective agreement. - Italy: Art 12 in the respective agreement. - Slovakia: Art 8 in the respective agreement. - Switzerland: Art 15 in the respective agreement. - Slovenia: Art 9 in the respective agreement. - Hungary: Art 11 and Art 12 in the respective agreement. - Czechia: Art 11 in the respective agreement.
Which LEAs can use this tool?	Police directorate; Directorate General for the Public Security.	- Art 41 para 1. and para. 4 Schengen Convention - Germany: Art 12 in the respective agreement. - Italy: Art 12 in the respective agreement. - Slovakia: Art 8 in the respective agreement. - Switzerland: Art 15 in the respective agreement. - Slovenia: Art 9 in the respective agreement. - Hungary: Art 11 and Art 12 in the respective agreement. - Czechia: Art 11 in the respective agreement.
What are the rules to be followed for the implementation of this tool?	The stakeholders involved vary slightly among the bilateral agreements. Police can apply the tool. The police directorate of the territory where the border is to be crossed must be informed as soon as possible. Also, the Directorate General for the Public Security, situated in the Ministry of Interior, must be informed.	- Art 41 para. 1 Schengen Convention - Germany: Art 12 in the respective agreement. - Italy: Art 12 in the respective agreement. - Slovakia: Art 8 in the respective agreement. - Switzerland: Art 15 in the respective agreement. - Slovenia: Art 9 in the respective agreement. - Hungary: Art 11 and Art 12 in the respective agreement. - Czechia: Art 11 in the respective agreement.
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Usually, no authorisation is necessary, since it lies in the nature of the tool that it has to be used instantly without the need of authorisation processes.	- Art 41 para 1. and para. 4 Schengen Convention - Germany: Art 12 in the respective agreement. - Italy: Art 12 in the respective agreement. - Slovakia: Art 8 in the respective agreement. - Switzerland: Art 15 in the respective agreement. - Slovenia: Art 9 in the respective agreement. - Hungary: Art 11 and Art 12 in the respective agreement. - Czechia: Art 11 in the respective agreement.
What ongoing supervision is required for the use of this tool?	The police directorate of the territory where the border is to be crossed must be informed as soon as possible. Also, the Directorate General for the Public Security, situated in the interior ministry, must be informed.	- Germany: Art 12 in the respective agreement. - Italy: Art 12 in the respective agreement. - Slovakia: Art 8 in the respective agreement. - Switzerland: Art 15 in the respective agreement. - Slovenia: Art 9 in the respective agreement. - Hungary: Art 11 and Art 12 in the respective agreement. - Czechia: Art 11 in the respective agreement.
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	- Code of Criminal Procedure (CCP). - Security Police Act (Sicherheitspolizeigesetz, SPG). - Agreement on the Cooperation in the Area of Witness Protection.	https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002326 https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10005792 https://www.parlament.gv.at/PAKT/VHG/XXV/I/I_00032/index.shtml
How is the tool defined?	On national level, there are two main pillars for witness protection. The CCP regulates witness protection in a criminal case. The SPG is the foundation for witness protection programmes. On international level, there is a multilateral agreement on cross-border cooperation with Bulgaria, Croatia, Czechia, Hungary, Poland, Slovakia and Slovenia. The	- Sections 156, 157, 158, 162, 165, 229 CCP. - Sections 21: para 1.21 para 2. 22 para. 1 subpara. 5 22 para. 2 SPG. - In general: Agreement on the Cooperation in the Area of Witness Protection.

Relevant items	Provisions	Sources used
	agreement does not affect national law and will hence only be discussed here in response to cross-border related questions due to consistency reasons. - CCP: Exemption from testifying (section 156); refusal to testify (sections 157/158); anonymous testimony (section 162); isolated testimony (can be reached by use of technical tools and thereby separating the hearings for witness testimonies from the hearings where suspects are present (section 165), by full exclusion of the public (section 229) or a combination of those two options). - SPG: Although witness protection programmes are possible in Austria, they are not specifically regulated by law. The only legal foundation for witness protection is written in the SPG. It allows police to protect people who can provide information about a dangerous attack or a criminal connection and are therefore particularly at risk, as well as any relatives of these people who may be at risk (section 22). The SPG also generally allows the police to avert dangers for the life, health and freedom of people (sections 21 and 22).	
For what types of crime can the tool be used?	None of the relevant tools relates to certain crime types as a condition for the use of the tool.	
Does national law allow this tool to be used in cross-border cases?	- CCP: As the tools concern the procedure of criminal court cases, there is no direct relevance for cross-border cases. - SPG: The SPG does not refer to cross-border cases, neither does it exclude them. - Agreement on the Cooperation in the Area of Witness Protection: The agreement mainly deals with the relocation of a witness from one to another country being party of the agreement. Once a witness has been relocated, the national witness protection regulations apply. Please refer to the respective areas for those regulations (CCP and SPG).	Especially Art. 1 and Art. 2 of the Agreement on the Cooperation in the Area of Witness Protection.
What thresholds must be passed for the use of this tool?	None of the relevant tools relates to certain crime types as a condition for the use of the tool.	
What types of stakeholder are involved in the implementation of this tool?	LEAs; Judicial Authority.	
Which LEAs can use this tool?	- CCP tools as part of a trial: To be used by prosecution in cooperation with judicial authority. They cannot actively choose to use or not to use the respective tools as they are mandatory law. - SPG: The tool can be used by police. - Agreement on the Cooperation in the Area of Witness Protection: The responsible authority on Austrian side regarding the agreement is the Federal Criminal Police Office.	- Sections from 153 CCP. - Section 4 SPG. - Agreement on the Cooperation in the Area of Witness Protection: Additional comments document, comment on Article 10. The Additional documents document can be found under the following link: https://www.parlament.gv.at/PAKT/VHG/XXV/I/I_00032/
What are the rules to be followed for the implementation of this tool?	- CCP: The relevant clauses can be applied for: - Persons who are to testify in the proceedings against a relative (sec. 156). - Relevant part: persons who would otherwise expose themselves or a relative to the risk of criminal prosecution (sec. 157). - Relevant part: persons, insofar as they otherwise expose themselves or a relative to the risk of direct and significant damage to their property (sec. 158). - Persons who would expose themselves to serious danger to life, health, physical integrity or freedom by disclosing their name and other personal details or by answering questions that allow conclusions to be drawn about them (sec. 162). - Victims particularly worthy of protection for various reasons (sec. 156, 229). - SPG: Section 21 SPG states: "The police must put an immediate end to dangerous attacks". There are no further requirements. Section 22 para. 1 subpara. 5 states: "The police is responsible for the special protection of people who can provide information about a dangerous attack or a criminal connection and are therefore particularly at risk, as well as any endangered relatives of these people". Section 22 para. 2 states: "The police must prevent dangerous attacks on life, health, freedom, morals, property or the environment if such attacks are likely."	- Sections 156, 157, 158, 162, 165, 229 CCP. - Sections 21: para 1.21 para 2. 22 para. 1 subpara. 5 22 para. 2 SPG.
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	- CCP: The tool particularly was designed to protect certain fundamental rights. - SPG: N/A.	- Sections: 156, 157, 158, 162, 165, 229, CCP. - Sections: 21 para. 2, 22 para. 1 subpara. 5, 22 para. 2, SPG.
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	- CCP: The tools are mainly provided by law and do not require explicit authorisation. - SPG: No authorisation is required according to the relevant law. It is likely that an approval by the Federal Criminal Police Office is required before applying the relevant clauses for the purpose of a witness protection programme. However, witness protection programmes are not formalised in Austrian law and this is only an estimation.	- Sections: 156, 157, 158, 162, 165, 229, CCP. - Sections: 21 para. 2, 22 para. 1 subpara. 5, 22 para. 2, SPG.
What ongoing supervision is required for the use of this tool?	N/A	

Relevant items	Provisions	Sources used
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	- There is no indication on organised crimes, only generic data. - Witness protection programme data: in general, in 2019, 50 national witness protection cases and 23 foreign witness protection cases were processed, of which 17 national protection cases and 14 foreign protection cases were closed.	Sicherheitsbericht 2019 Kriminalität (Security Report 2019 Crime) Page 62. https://www.bmi.gv.at/508/files/SIB_2019/1_SIB_2019_Hauptteil_V20200817_pr_aes.pdf
Surveillance		
Relevant documents (legal and non-legal) that define the functioning of the tool	- Code of Criminal Procedure (CCP) (Strafprozessordnung) - Surveillance in cross-border settings is also regulated in bilateral agreements with the bordering countries. However, the CCP as dominating and most relevant legal foundation shall suffice as a reference here for consistency reasons.	https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002326
Specific range of application of the tool	- Tracking surveillance: locating a technical device. - Visual surveillance. - Acoustic surveillance. - Intercepting mails. - Surveillance of messages.	Sections 130 (general), 133 (general), 134 (definitions), 135 (tracking, messages), 136 (visual, acoustic), 137 (general), 138 (general) CCP.
How is the tool defined?	- Tracking: Use of technical means to determine geographical locations and the number used for the international identification of the user (IMSI). - Visual and acoustic surveillance: Surveillance of the actions of persons, breaking through their private sphere, and of the communications of persons not intended for the direct knowledge of third parties, using technical means for the transmission of images or sounds and for the recording of images or sounds without the knowledge of the persons concerned. - Intercepting mails: Opening and withholding telegrams, letters or other items sent by or addressed to the suspect. - Surveillance of messages: Monitoring of messages and information sent by an individual via a communications network or an information technology service.	- Tracking: section 134 para. 2a CCP. - Visual/acoustic: section 134 para. 4 CCP. - Intercepting mails: section 134 para. 1 CCP. - Surveillance of messages: section 134 para. 3 CCP.
For what types of crime can the tool be used?	Cross crime areas. Section 130 para. 1 CCP states: Surveillance is permissible if it appears necessary to solve a criminal offence or to find out the whereabouts of the suspect.	Section 130 para. 1 CCP.
Does national law allow this tool to be used in cross-border cases?	Basically, the tool can also be used in a cross-border setting. However, the CCP restricts the use of the tool outside of Austrian territory as follows: "If the surveillance tool is being conducted outside of Austrian territory, it can only be applied if there is the suspicion of an intentionally committed criminal offence punishable by more than one year of imprisonment and it can be assumed on the basis of certain facts that the person under surveillance has committed the offence or will establish contact with the suspect or that the whereabouts of a fugitive or absent suspect can be determined".	Section 130 para. 3 subpara. 3 CCP.
What thresholds must be passed for the use of this tool?	- Section 130 para. 1 CCP states: Surveillance is permissible if it appears necessary to solve a criminal offence or to find out the whereabouts of the suspect. - Therefore, no specific terms of imprisonment are tied to the tool and imprisonment times theoretically can range up to life imprisonment.	Section 130 para. 1 CCP.
What types of stakeholder are involved in the implementation of this tool?	LEAs; Judicial Authority.	- Section 133 CCP. - Section 137 CCP.
Which LEAs can use this tool?	Criminal Police; Public Prosecution.	- Section 133 CCP. - Section 137 CCP.
What are the rules to be followed for the implementation of this tool?	- General: If the surveillance tool contains geographical tracking of the person, is being conducted for a time lasting longer than 48 hours or is being conducted outside of Austrian territory, it can only be applied if there is the suspicion of an intentionally committed criminal offence punishable by more than one year's imprisonment and it can be assumed on the basis of certain facts that the person under surveillance has committed the offence or will establish contact with the suspect or that the whereabouts of a fugitive or absent suspect can be determined. - Tracking surveillance can generally only be used, if the observation would otherwise be unpromising or substantially difficult. Specifically, it can only be used in the case of kidnapping; if a crime that is punishable with a least one year imprisonment is likely to be solved by the tool; or if the whereabouts of a fugitive person who is threatened with more than one year imprisonment can be identified. - Visual and acoustic surveillance is permitted in cases of: kidnapping; in the case that it is limited to events and statements that are intended for the knowledge of an undercover investigator; or if the investigation of a crime punishable by more than ten years' imprisonment, an offence under sections 278a to 278e of the Criminal Code or the investigation or prevention of acts committed within the framework of a criminal organisation or a terrorist organisation or the investigation of the whereabouts of a	- Section 130 para. 3 CCP. - Section 130 para. 2 CCP. - Section 135 para. 2a and 2 CCP. - Section 136 para. 1 CCP. - Section 135 para. 1 CCP. - Section 135 para. 2 CCP

Relevant items	Provisions	Sources used
	person convicted of one of the offences mentioned above would otherwise be futile or substantially impeded. - Intercepting mails is permitted, if it is necessary for the investigation of an offence committed with intent and punishable by more than one year imprisonment. - Surveillance of messages is permitted, in the case of kidnapping; if a crime that is punishable with a least one year imprisonment is likely to be solved by the tool; or if the whereabouts of a fugitive person who is threatened with more than one year imprisonment can be identified.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	- Basically, the criminal police can carry out surveillance on its own initiative. - Order by the prosecution is needed if: The surveillance tool contains geographical tracking of the person, is being conducted for a time lasting longer than 48 hours or is being conducted outside of Austrian territory, it can only be applied if there is the suspicion of an intentionally committed criminal offence punishable by more than one year imprisonment and it can be assumed on the basis of certain facts that the person under surveillance has committed the offence or will establish contact with the suspect or that the whereabouts of a fugitive or absent suspect can be determined. - Authorisation by a court and order by the prosecution is needed: For all cases of visual/acoustic surveillance except kidnapping.	- Section 133 CCP. - Section 137 CCP.
What ongoing supervision is required for the use of this tool?	Besides the authorisation chain, there is no indication for continuous supervision in case the tool comes to use.	
Is there any national case law relating to the use of this tool in cross-border crime cases?	Date: 29 October 2014. Summary: The case concerns a suspect who was accused of illegal drug trafficking by the Dutch authorities. The Dutch authorities asked the Austrian authorities to provide acoustic surveillance. The Austrian public prosecutor's office had only authorised the surveillance after the surveillance had taken place. This was found to be illegal by the Austrian courts.	European Case Law Identifier (ECLI) ECLI:AT:OGH0002:2014:0150OS00180.13D.1029.000 https://www.ris.bka.gv.at/JustizEntscheidung.wxe?Abfrage=Justiz&Dokumentnummer=JIT_20141029_OGH0002_0150OS00180_13D0000_000&IncludeSelf=True
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	In 2019, 177 cases of optical and acoustic surveillance were documented. 3.525 cases of message surveillance were documented. 175 cases of tracking a technical device were documented.	Sicherheitsbericht 2019 (Security Report 2019) https://www.bvt.gv.at/bmi_documents/2563.pdf
Undercover / covert operations		
Relevant documents (legal and non-legal) that define the functioning of the tool	- Code of Criminal Procedure (CCP) (Strafprozessordnung) - Covert operations in cross-border settings are also regulated in bilateral agreements with the bordering countries. However, the CCP as dominating and most relevant legal foundation shall suffice as a reference here for consistency reasons.	https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002326
How is the tool defined?	There are two tools for the purpose of undercover operations: Covert investigations and fictitious purchases.	Sections 131 (covert investigations) and 132 (fictitious purchases) CCP.
For what types of crime can the tool be used?	Cross crime areas. Covert investigations are permitted if they appear necessary to solve a criminal offence. Fictitious purchases are permitted for the purpose of solving a crime or for securing objects or assets.	Sections 131 (covert investigations) and 132 (fictitious purchases) CCP.
Does national law allow this tool to be used in cross-border cases?	N/A	
What thresholds must be passed for the use of this tool?	- Covert investigations are permitted if they appear necessary to solve a criminal offence. - Fictitious purchases are permitted for the purpose of solving a crime or for securing objects or assets. - Therefore, no specific terms of imprisonment are tied to the tools and imprisonment times theoretically can range up to life imprisonment. - However, systematic covert investigations carried out over a longer period of time are only admissible if the solving of a criminal offence committed intentionally and punishable by more than one year's imprisonment or the prevention of a criminal offence planned within the framework of a criminal or terrorist association or a criminal organisation would otherwise be substantially more difficult.	Sections 131 (covert investigations) 132 (fictitious purchases) CCP.
What types of stakeholder are involved in the implementation of this tool?	LEAs.	Section 133 CCP.
Which LEAs can use this tool?	Criminal Police; Public Prosecution.	Section 133 CCP.
What are the rules to be followed for the implementation of this tool?	Covert investigations that are not carried out systematically and over a longer period of time can be carried out by the police without further authorisation. Other investigations must be ordered by the public prosecution.	Section 133 CCP.

Relevant items	Provisions	Sources used
	Fictitious purchases must be ordered by the public prosecution, except if the purchase serves to secure drugs or counterfeit money.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Please refer to the analysis above.	
What ongoing supervision is required for the use of this tool?	Besides the authorisation chain, there is no indication for continuous supervision in case the tool comes to use.	
Is there any national case law relating to the use of this tool in cross-border crime cases?	Date: 23 July 2008. Summary: The case deals with cross-border drug trafficking and drug dealing in Austria. A substantial drug amount was sold to a covert investigator in the setting of a fictitious purchase. The seller claimed he was provoked and induced by the investigator to make the sale (which is illegal in Austria) and eventually lost the case.	European Case Law Identifier (ECLI) ECLI:AT:OGH0002:2008:0130OS00073.08X.0723.000 https://www.ris.bka.gv.at/Dokument.wxe?ResultFunctionToken=52153e4e-50c6-4394-8c52-627d5419678e&Position=1&SkipToDocumentPage=True&Abfrage=Justiz&Gericht=&Rechtssatznummer=&Rechtssatz=&Fundstelle=&AenderungenSeit=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=&VonDatum=&BisDatum=01.03.2021&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=%27132+stpo%27&Dokumentnummer=JJT_20080723_OGH0002_0130OS00073_08X0000_000
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	Code of Criminal Procedure (CCP) (Strafprozessordnung)	https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002326
Specific range of application of the tool	- Informants are not explicitly named by Austrian law. However, the CCP defines "covert investigation" as the use of criminal police agents or other individuals on behalf of the criminal police, who do not reveal their official position or mandate. - The wording "other individuals" ("andere Personen" in the German original phrasing) hence allows any type of informant.	Section 129 para. 2 CCP.
How is the tool defined?	Covert investigation.	Section 131 CCP.
For what types of crime can the tool be used?	Cross crime areas. Covert investigations are permitted if they appear necessary to solve a criminal offence.	Section 131 CCP.
Does national law allow this tool to be used in cross-border cases?	N/A	
What thresholds must be passed for the use of this tool?	- Covert investigations are permitted if they appear necessary to solve a criminal offence. Fictitious purchases are permitted for the purpose of solving a crime or for securing objects or assets. - Therefore, no specific terms of imprisonment are tied to the tools and imprisonment times theoretically can range up to life imprisonment. - However, systematic covert investigations carried out over a longer period of time are only admissible if the solving of a criminal offence committed intentionally and punishable by more than one year's imprisonment or the prevention of a criminal offence planned within the framework of a criminal or terrorist association or a criminal organisation would otherwise be substantially more difficult.	Section 131 CCP.
What types of stakeholder are involved in the implementation of this tool?	LEAs.	Section 133 CCP.
Which LEAs can use this tool?	Criminal Police; Public Prosecution.	Section 133 CCP.
What are the rules to be followed for the implementation of this tool?	Covert investigations that are not carried out systematically and over a longer period of time can be carried out by the police without further authorisation. Other investigations must be ordered by the public prosecution.	Section 133 CCP.
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Please refer to the analysis above.	

Relevant items	Provisions	Sources used
What ongoing supervision is required for the use of this tool?	Besides the authorisation chain, there is no indication for continuous supervision in case the tool comes to use.	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	

Source: Author's own elaboration

Belgium

Table 19 – Overview of national rules on investigative tools - Belgium

Relevant items	Provisions	Sources used
Controlled Delivery		
Relevant documents (legal and non-legal) that define the functioning of the tool	Royal decree of 09-04-2003 regarding police investigation techniques (art. 5 and art.6).	http://www.ejustice.just.fgov.be/eli/bsluit/2003/04/09/2003009348/justel
How is the tool defined?	- Controlled delivery (art. 5): Controlled delivery is the technique used by a police force, whereby an illegal transport of goods or persons, of which the police services are aware and police officers themselves carry out and deliver the illegal transport, or provide assistance for this, is allowed to pass under the permanent control of the police services, and where the police intervention is postponed at the latest until the final destination, in Belgium or abroad. - Controlled onward delivery (art. 6): The controlled onward delivery is the technique used by a police force, whereby an illegal transport of goods, of which the police forces are aware and police officers themselves carry out and deliver the illegal transport, or provide assistance for this, is allowed to pass under the permanent control of the police forces, without a police intervention at the latest at the final destination. The controlled transfer of persons is not permitted.	http://www.ejustice.just.fgov.be/eli/bsluit/2003/04/09/2003009348/justel
For what types of crime can the tool be used?	Controlled delivery / controlled onward delivery can be used in the following cases: - Art. 324bis Criminal Code dd. 08-06-1867: By criminal organisation is meant any structured association of more than two persons that lasts over time, with the aim of committing by mutual agreement crimes and offenses punishable by imprisonment of three years or a more severe sentence, in order to obtain direct or indirect capital gains. - Art. 90ter §2-§4 Code of Criminal Procedure dd. 17-11-1808: List of crimes with reference to Criminal Code dd. 08-06-1867.	- Criminal Code: http://www.ejustice.just.fgov.be/eli/wet/1867/06/08/1867060850/justel - Code of Criminal Procedure: http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
Does national law allow this tool to be used in cross-border cases?	The authorities of the countries concerned, the countries where the shipment passes and the country of final destination must be notified in advance by the authority from which the controlled consignment originates. The competent authorities of the countries concerned must also have given their consent in writing before the operation is allowed to start.	Agreement established by the Council in accordance with Article 34 of the Treaty on European Union, on mutual legal assistance in criminal matters between the Member States of the European Union, 29 May 2000. http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2000052937&table_name=wet
What thresholds must be passed for the use of this tool?	Controlled delivery / controlled onward delivery can thus only be used for crimes committed by a criminal organisation (art. 324bis Criminal Code dd. 08-06-1867) or for a limited list of crimes (art. 90ter §2-§4 Code of Criminal Procedure dd. 17-11-1808)	- Criminal Code: http://www.ejustice.just.fgov.be/eli/wet/1867/06/08/1867060850/justel - Code of Criminal Procedure: http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
What types of stakeholder are involved in the implementation of this tool?	- Public Prosecutor: The public prosecutor is responsible for permanent control over the application of the special investigation methods by the police services within his judicial district. - Federal Prosecutor: The public prosecutor informs the federal prosecutor of the special investigative methods used in his judicial district. If the application of the special investigation methods extends over several judicial districts or falls within the competence of the federal prosecutor, the competent public prosecutors and the federal prosecutor shall immediately inform each other and take all necessary measures to ensure the proper conduct of the proceedings to insure the operation. - Federal Police: For each decentralised judicial directorate, an officer is charged with permanent control over the special investigative methods in the district.	Art. 47ter Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
Which LEAs can use this tool?	Special Investigation methods (observation, infiltration and use of informants) are carried out by the judicial directory of the Federal Police.	Directive of 20-02-2002 regulating the division of tasks, cooperation, coordination and integration between the local and federal police in the tasks of judicial police

Relevant items	Provisions	Sources used
	In Belgium a 'controlled delivery' is not an investigative tool in itself, it is an investigative technique used during an infiltration. Other investigative techniques used during an infiltration are a pseudo-purchase, a trust purchase, a test purchase, a pseudo-sale, a trust sale and a front store. (See below)	http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=200202031&table_name=wet
What are the rules to be followed for the implementation of this tool?	- Controlled (onward) delivery can only be used when an Infiltration is already ongoing. - There are four basic principles underlying the special investigation methods and techniques of the police: 1. Subsidiarity: This means that the methods are only to be employed, if the investigation, according to the facts, requires it and if the other means of investigation do not seem to be sufficient, which is decided a priori and in abstract to by the magistrate who authorizes it. There is no requirement for the classic investigation methods to actually be tested - or that one must await the failure of the classic detection techniques before using a special method. 2. Proportionality: this implies that the used method should be proportional to the severity of the crime and it implies the chosen method should be proportionate to the goal. The limitation or breach of individual rights and freedoms can only be allowed in case of one serious breach of the legal order. Proportionality also means that before the action begins, there should be objective data that strongly suggest that the target individuals are committing criminal acts or are about to do so. So-called fishing expeditions or exploratory operations with use of undercover techniques are therefore excluded. 3. Non-provocation: When implementing a special investigation method, a police officer may not bring a suspect to commit other criminal offenses than those on which his intent was previously aimed. In case of violation, the criminal action is declared inadmissible with regard to these facts. 4. Prohibition to commit crimes: Crimes committed by police officers: The police officer charged with carrying out the special investigative methods is prohibited from committing criminal offenses in the context of his assignment. Police officers who, in the context of their assignment and with a view to its success or in order to ensure their own safety or that of other persons involved in the operation, remain free from punishment, commit strictly necessary criminal offenses, provided explicitly agreement of the public prosecutor. Those offenses must not be more serious than those for which the methods are used and must necessarily be proportionate to the aim pursued.	- Art. 47quater Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel - Art. 47quinquies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel https://bib.kuleuven.be/rbib/collectie/archieven/vigiles/2004-2-40-63.pdf
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool?	- The public prosecutor can authorize an infiltration in the context of the criminal investigation if the investigation so requires and the other means of investigation do not appear to be sufficient to reveal the truth. He can authorize the police service, within the legal framework of an infiltration and with due observance of its purpose, to use certain police investigation techniques. The public prosecutor can also, if there is reason to do so, grant permission to take the necessary measures to safeguard the security and the physical, psychological and moral integrity of the undercover officer. - The authorisation for infiltration is in writing and states: 1. The serious indications of the criminal offense that justify the infiltration or, if the infiltration is part of the proactive investigation the reasonable suspicion that it has been committed or has already been committed but has not yet been discovered offenses committed, and the special instructions relating to the elements described in this last provision, justifying the infiltration. 2. The reasons why the infiltration is indispensable to reveal the truth. 3. If known, the name or otherwise a description as accurate as possible of the person or persons referred to. 4. The manner in which the infiltration will be carried out, including the permission to briefly call on the expertise of a citizen and the admission of police investigation techniques to use. 5. The period during which the infiltration can be carried out and which may not exceed three months from the date of the authorisation. 6. The name and capacity of the judicial police officer who is in charge of carrying out the infiltration. - At that time, the public prosecutor will state in a separate written decision the crimes that can be committed by the police forces, in the context of the infiltration. - The public prosecutor can always change, supplement or extend his authorisation to infiltrate in a motivated manner. He can revoke his authorisation at any time. He verifies with every amendment, addition or extension of his authorisation whether the conditions stipulated have been fulfilled.	- Art. 47octies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel - Art. 9 Royal decree of 09-04-2003 regarding police investigation techniques

Relevant items	Provisions	Sources used
	- The public prosecutor is responsible for the enforcement of the authorisations for infiltration granted by the investigating judge in the context of a judicial investigation. - The police investigation techniques of the controlled delivery of persons and of the controlled onward delivery require the prior written agreement of the federal prosecutor. In case of controlled delivery of persons and controlled onward delivery, this agreement can be provided verbally in urgent circumstances. The agreement will be confirmed in writing as soon as possible.	
What ongoing supervision is required for the use of this tool?	- The officer of the judicial police will report accurately, completely and truthfully in writing to the Public Prosecutor on each stage in the execution of the infiltrations under his control. These confidential reports are sent directly to the Public Prosecutor, who keeps them in a separate and confidential file. He has sole access to this file, without prejudice to the right of inspection of the investigating judge and of the indictment chamber. The content of this file is covered by professional secrecy. - The authorisation to infiltrate and the decisions to amend, supplement or extend are attached to the confidential file. The officer of the judicial police draws up an official report of the different phases of the execution of the infiltration, but does not mention any elements that prevent the protection of the technical aids and the police investigation techniques used, whether the safeguarding of the security and the protection of the identity of the informant, the police officers charged with carrying out the infiltration can jeopardize. These elements are only included in the written report. - An official report refers to the authorisation to infiltrate. The public prosecutor confirms by written decision the existence of the authorisation for infiltration granted by him. The reports drawn up shall be added to the criminal file no later than after the infiltration has been completed. - At least every three months, the Public Prosecutor sends all files in which he has applied the special investigation methods (observation, infiltration and civilian infiltration) and in which he has decided not to prosecute, to the Attorney General in order to enable them to verify the legality of the methods used. The Attorney General reports on this check. This report also deals with the application of the special investigative methods in the context of the execution of sentences or deprivation of liberty measures in its jurisdiction. The report is sent to the Board of Attorney General, which includes the global evaluation and the statistical data relating to these reports in its annual report. In his annual report, the federal prosecutor publishes the global evaluation and the statistical data of the files in which he has applied the special investigation methods (observation, infiltration and civilian infiltration) and in which he has decided not to prosecute. This report also deals with the application of the special investigative methods in the context of the execution of sentences or deprivation of liberty measures for federal criminal files.	- Art. 47novies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel - Art. 47undecies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Data available on the number of times this tool has been used for SOC cases	- Controlled delivery persons: 0 in 2016, 1 in 2017 and 0 in 2018. - Controlled onward delivery goods: 0 in 2016, 0 in 2017 and 0 in 2018. - Guarded delivery persons: 0 in 2016, 0 in 2017 and 1 in 2018. - Guarded onward delivery goods: 1 in 2016, 0 in 2017 and 4 in 2018.	rapport annuel 2018 alpha-nl.pdf (om-mp.be)
Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	- MARCH 28, 2014 - Ministerial guideline MFO-7 on the management of dynamic unplanned events triggering an immediate and coordinated supra-local police response - Hot pursuit is not defined in national law. It is an intervention technique used by the police.	
How is the tool defined?	"Dynamic event" is understood to mean an event that evolves in space and time. This mainly concerns situations of hot pursuit	MARCH 28, 2014 - Ministerial guideline MFO-7 on the management of dynamic unplanned events triggering an immediate and coordinated supra-local police response http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2014032832&table_name=wet
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross-border cases?	- Treaty of 08-06-2004 between the Kingdom of the Netherlands, the Kingdom of Belgium and the Grand Duchy of Luxembourg regarding cross-border police intervention - According to Belgian law, hot pursuit is not an investigation method (not included in Code of Criminal Procedure). - For the conduct of the cross-border pursuit, the provisions of Article 41 of the implementing the Schengen Agreement shall apply, provided that:	Art. 18 Treaty of 08-06-2004 between the Kingdom of the Netherlands, the Kingdom of Belgium and the Grand Duchy of Luxembourg regarding cross-border police intervention http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2004060848&table_name=wet

Relevant items	Provisions	Sources used
	a) A cross-border chase may continue, in accordance with national law, if it concerns persons who have escaped custodial sentence or are suspected of an offense liable to give rise to extradition. b) The right of hot pursuit referred to in Article 41, paragraph 1, of the Convention implementing the Schengen Agreement is exercised in the territory of the other Contracting Party, without any limitation expressed in distance or in time and granting the right to arrest the person being pursued. c) The pursuit can also take place, in accordance with national law, in airspace and on sea and waterways. d) Otherwise, if there is reason to do so, action will be taken in accordance with Article 26 of the Convention on Extradition and Mutual Assistance in Criminal Matters between the Kingdom of the Netherlands, the Kingdom of Belgium and the Grand Duchy of Luxembourg, even if the letters rogatory referred to therein is not present.	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	The operational direction and coordination of missions, the execution of which extends over the territory of more than one police zone, are entrusted to a designated police chief on the basis of an agreement, or the DirCo, in case of joint action by different local police forces and of the federal police, unless the competent local and federal authorities decide otherwise. In the context of unplanned events, the police chief / DirCo is not always able to immediately perform his / her tasks of leadership and coordination. Nevertheless, in this initial phase, hereinafter referred to as the "reflex phase", a number of crucial decisions arise. By analogy with emergency management, a clear response schedule must be drawn up in advance. In order to ensure effective operational cooperation and integrated police action, this circular sets out the framework in which this "first-line" police action should take place. The principles and modalities contained in this circular do not affect the powers assigned to the judicial director (DirJud). See Below for all stakeholders	MARCH 28, 2014 - Ministerial guideline MFO-7 on the management of dynamic unplanned events triggering an immediate and coordinated supra-local police response http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2014032832&table_name=wet
Which LEAs can use this tool?	Police.	
What are the rules to be followed for the implementation of this tool?	- The effectiveness of operational management and coordination, integrated policing and a tailor-made approach depend, among other things, on judicious organisation and use of resources. A good practice in this area is to work by analogy with the Gold-Silver-Bronze structure, which is already established in the negotiated management of public space. - The police force that is the first to be confronted with the dynamic unplanned event takes the necessary urgent measures on the initiative, based on its own analysis or evaluation of legality / subsidiarity / proportionality / appropriateness. If the cognizance takes place via a police team on site, this team immediately informs the competent CIC in the routine discussion group (9) and passes on all essential elements of information. If it concerns a police force with an autonomous local dispatching, the CIC will be notified via this local dispatching. In this case too, the "immediacy" of the notification is crucial. As soon as possible, the CIC will inform a pre-defined person (present on site) from the police force (10); the National Incident Point (NIP); according to the agreements and modalities of the intervention policy (GPI 49); the police chief; the DirCo; the DirJud; from where the event started. - The NIP assesses the possibility and expediency of deploying specialised support services (air support, dog support) and initiates them, if necessary. - As Gold Commander, the Chief of Police or DirCo bears overall operational final responsibility for the police action taken. In the reflex phase, the operational management powers are exercised by the relevant control room (the CIC or the autonomous local dispatching), which acts as Silver Commander. The control room is the service within the police that has the necessary information and the required overview to determine the most appropriate measures and to pass them on to the teams on the field. Starting from the principles of legality / subsidiarity / proportionality / expediency, the environmental factors (built-up areas, motorways), weather conditions, the presence of other road users, the risks to the safety of the intervening police officers and other citizens (speed, wrong-way driving of the fleeing vehicle, driving on the hard shoulder, ..) are also taken into account. The NIP and the CIC will always test their assessment and rely on a decision matrix that has been developed for situations of chasing and intercepting vehicles. This matrix is part of the intervention tactics. Tactical command (Bronze Commander) is generally exercised by the police team which, in the chronology of events, is the first vehicle involved in the pursuit (13). In operations that take place in the specific field of action of the federal road police (motorways), this tactical command is performed as a priority by a team of the federal road police.	- Question nr. 5-2765 d.d. 15 juli 2011 to the Minister of Home Affairs https://www.senate.be/www/?MIval=/Vragen/SVPrint&LEG=5&NR=2765&LANG=nl - MARCH 28, 2014 - Ministerial guideline MFO-7 on the management of dynamic unplanned events triggering an immediate and coordinated supra-local police response http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2014032832&table_name=wet

Relevant items	Provisions	Sources used
	- The traffic regulations stipulate that the provisions on speed limits do not apply to vehicles used by authorised persons, nor to priority vehicles when justified by an urgent order. Hot pursuit, with a view to interception, can be regarded as an urgent task. - The general rules of conduct of the traffic regulations impose a duty of caution on every driver. It stipulates that drivers must adapt their speed to the conditions, in particular the presence of other road users, weather conditions, location, obstructions, traffic density, visibility, road conditions and the load of their vehicle. Traffic regulations do not exempt the police from this duty of caution.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	Code of Criminal Procedure Title VIIter Protection of threatened witnesses Art. 102-111decies.	http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
How is the tool defined?	1) Threatened witness: a person who is at risk as a result of statements made or to be made in the course of the criminal investigation or judicial investigation in the context of a criminal case, either in Belgium or before an international court or, when reciprocity is guaranteed in this respect is abroad, and who is willing to confirm those statements in court if requested. 2) Family members: the spouse of the threatened witness or the person with whom he lives and has a lasting affective and sexual relationship, the live-in relatives of the threatened witness, of his spouse or of the person he lives with and a lasting affective and are in a sexual relationship, their adoptive and adopted children living at home and the blood relatives of their adopters and adopted children living at home. 3) Other blood relatives: non-resident relatives up to the third degree of the threatened witness, of his spouse or of the person with whom he lives and has a lasting affective and sexual relationship, their non-resident adopters and adopted children and the non-resident - Residing relatives of their adopters and adopted children up to the second degree.	Art.102-111decies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
For what types of crime can the tool be used?	Normal protective measures in all cases. Special protective measures for crimes listed in Art.90ter §2-§4 Of the Code of Criminal Procedure or 324bis of the Criminal Code.	Art.102-111decies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
Does national law allow this tool to be used in cross-border cases?	When reciprocity is guaranteed, the witness can stay abroad. It is a bilateral agreement.	Art.102-111decies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
What thresholds must be passed for the use of this tool?	No Limitations.	
What types of stakeholder are involved in the implementation of this tool?	The Witness Protection Commission is authorised to grant, amend and withdraw protective measures and financial aid measures. The Witness Protection Commission is composed of the Federal Prosecutor, who serves as Chairman, a Public Prosecutor appointed by the Council of Public Prosecutors, the Attorney General who has been assigned the specific role of international relations, the Director General of Judicial Police of the Federal Police, the Director-General for Operational Support of the Federal Police, a representative from the Ministry of Justice and a representative from the Ministry of the Interior. The latter two have only advisory powers and do not have the right to vote. The Witness Protection Commission meets when convened by its chairman. The members of the Witness Protection Commission are present in person or have themselves replaced in accordance with the rules they lay down in the internal regulations. The King approves the committee's internal regulations. The protection is coordinated by the Witness Protection Service at the General Directorate of Judicial Police of the federal police. The implementation of the protection of detainees within the prison is carried out by the Directorate-General of Penal Institutions. In	Art.102-111decies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel

Relevant items	Provisions	Sources used
	all other cases, the enforcement of the protection is assured by the General Directorate for Operational Support of the federal police. The Witness Protection Commission may, with due observance of the principles of subsidiarity and proportionality, grant ordinary protective measures to a threatened witness and, where appropriate and insofar as they are at risk as a result of the statements made or to be made by him his family members and other blood relatives. Common protective measures may include, in particular: 1) Shielding the data of the person concerned from the population and civil registry services. 2) Providing advice in the field of prevention. 3) The placement of techno-preventive means. 4) Appointing a liaison officer. 5) Providing for an alarm procedure. 6) Providing psychological assistance. 7) Preventive patrolling by the police services. 8) Registering incoming and outgoing calls. 9) Regularly checking the consultations of the national register and / or shielding the data of the person concerned. 10) Providing a secret telephone number. 11) Making a protected number plate available. 12) Making a mobile phone available for emergency calls. 13) Immediate and close physical protection of the person concerned. 14) Electronically securing the person concerned. 15) Relocating the person concerned for a maximum of 45 days. 16) Placing the detainee concerned person in a particularly secure section of the prison. 17) Registering at a contact address in deviation from the law of 19 July 1991 on population registers, identity cards, alien cards and residence documents and amending the law of 8 August 1983 regulating a National Register of natural persons. The person to whom special protection measures are granted has the right to be safeguarded from his social and administrative rights. The federal prosecutor can request the cooperation of the officials and agents of the public services and administrations for this purpose. The witness protection service is responsible for the implementation of this claim. Any person who, by virtue of his position, becomes aware of these measures or who cooperates with them, is obliged to observe secrecy. Any violation of secrecy will be punished in accordance with Article 458 of the Criminal Code. In addition, the Witness Protection Commission, with due regard for the principles of subsidiarity and proportionality, can only grant special protection measures to an endangered witness whose protection cannot be ensured by ordinary protective measures and whose statements relate to a crime as referred to in Article 90ter, §§ 2, 3 or 4, a crime committed within the framework of a criminal organisation as referred to in Article 324bis of the Criminal Code or a crime as referred to in the Act of 16 June 1993 on the punishment of serious violations of international humanitarian law, and, where appropriate, case, to his family members and, in so far as they are endangered as a result of the statements made or to be made by him, to his other blood relatives. The special protective measures may include: 1) Relocating the person concerned for more than 45 days. 2) Changing the identity of the person concerned. 3) Assigning a temporary protection identity and the strictly necessary documents to support it to the person concerned. The temporary protection identity concerns the surname, first names, date and place of birth of the person concerned. Its allocation is revocable and cannot lead to legal consequences. There can be no crime when strictly necessary facts in that regard are committed to ensure the protection of the witness. If the Witness Protection Commission proposes the special protection measure referred to in Article 104, § 2, second paragraph, 2 °, the Minister of Justice may, in a first ministerial order, change the name, first names, date and place of birth of the person concerned. permit, notwithstanding the provisions of Book I, Title II and Title VIII / 1, Chapter 3, of the Civil Code. The identity change procedure is only applied to persons who have Belgian nationality. The new identity will be established on the basis of a proposal from the Witness Protection Service, after consultation with the person concerned or his legal representative, and will be communicated to the Minister of Justice, who will include it in a second ministerial decision, after approval by the chairman of the Witness Protection Commission. The chairman of the Witness Protection Commission requests the registration of the following notification on the civil status certificates of the beneficiaries with their old identity in the Database of Civil Registry, referred to in Title II, Chapter 3, of the Civil Code. and to civil status certificates relating to the children of the beneficiaries born during the change of identity procedure: "Article 106 of the Code of Civil Procedure - permission granted to change data on civil status - Original name and first name:	

Relevant items	Provisions	Sources used
	(beneficiary)". For each notification referred to in the first paragraph, a similar notification will be made in the National Register of natural persons. No copy or extract of civil status certificates bearing the old identity of the beneficiary may be issued. The chairman of the Witness Protection Commission designates the municipalities that are charged with drawing up the certificates of civil status as referred to in paragraph 4. These municipalities then appoint, in consultation with the Witness Protection Service, the authorised officer of the municipal administration. Within ten days after the signing of the second ministerial order referred to in paragraph 1, third paragraph, the original of that order will be sent to the Witness Protection Service. The latter will inform the chairman of the Witness Protection Commission, who will then request the registrar of births, deaths and marriages appointed by him to draw up the certificates of civil status in the Database of Civil Registry Deeds. The new data from the registry office will have effect on the day the deed is drawn up. The new identity of the beneficiaries is registered in the National Register of natural persons. The Witness Protection Service keeps the originals of the claims and the ministerial decisions referred to in this article. No copy or extract of the claims and of the ministerial orders referred to in this article may be issued or kept by the municipal authorities. The Witness Protection Commission can, taking into account the specific situation of the person concerned, grant financial assistance measures to the threatened witness to whom special protective measures are granted. The public prosecutor, the attorney general, the federal prosecutor or the investigating judge, as the case may be, may request the granting of protective measures and financial aid measures in a reasoned application, accompanied by a copy of the file. As soon as the chairman of the Witness Protection Commission has received the petition for the granting of protective measures and, if necessary, financial aid measures, he asks the Director-General for Judicial Police of the Federal Police for a written opinion. The decision of the Witness Protection Commission is reasoned. If the decision concerns a change of identity, it will be communicated to the Minister of Justice. The federal prosecutor can also, if there are grounds to do so, grant permission to take the necessary preventive supervision measures to safeguard the safety and physical, psychological and moral integrity of the persons referred to in Article 102 after granting protective measures such as referred to in paragraphs 1 and 2. The threatened witness will be notified in writing of the possibility to do so. In 2019 Art111bis-decies was added to describe the protection of witnesses with a public position.	
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	See above	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	See above	
What ongoing supervision is required for the use of this tool?	See above	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	2018: 1 extra person in witness protection in Belgium and 1 aid request from abroad regarding witness protection.	rapport annuel 2018 alpha-nl.pdf (om-mp.be)
Surveillance		
Relevant documents (legal and non-legal) that define the functioning of the tool	Code of Criminal Procedure dd. 17-11-1808, section III Special Investigation Methods, subsection 3 Observation (observation = surveillance).	http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
Specific range of application of the tool	A technical aid is defined as: 'A technical aid within the meaning of this Code is a configuration of components that detects signals, transports them, activates their registration and records the signals, with the exception of the technical means used to implement a measure as referred to in Article 90ter.'. Article 90ter refers to intercepting, reading, searching and recording communications or data from a computer system or part of it that are not accessible to the public by technical means or extend the search in a computer system or part of it.	Art. 47sexies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
How is the tool defined?	Observation within the meaning of this code is the systematic observation by a police officer of one or more persons, their presence or behaviour, or of certain things, places or events. A systematic observation within the meaning of this Code is an observation of more than five consecutive days or of more than five non-consecutive days spread over a period of one month,	Art. 47sexies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel

Relevant items	Provisions	Sources used
	an observation in which technical aids are used, an observation with an international character, or an observation carried out by the specialised units of the federal police.	
For what types of crime can the tool be used?	The public prosecutor can authorize an observation within the framework of the criminal investigation if the investigation so requires and the other means of investigation do not appear to be sufficient to reveal the truth. An observation using technical aids can only be authorised if there are serious indications that the criminal offenses may result in a correctional prison sentence of one year or a heavier sentence. No further limits apply, i.e. covers all crime types.	Art. 47sexies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
Does national law allow this tool to be used in cross-border cases?	For the purposes of cross-border surveillance, the provisions of Article 40 of the Convention implementing the Schengen Agreement shall apply, provided that: - The surveillance carried out in accordance with Article 40, paragraph 1, of the Convention implementing the Schengen Agreement, subject to national law, may be extended to persons who have avoided a custodial sentence imposed for committing a criminal offense. fact that could lead to extradition, or to persons who could lead to the discovery of those persons. - The surveillance is carried out under the general conditions referred to in Article 40, paragraph 3, of the Convention implementing the Schengen Agreement, on the understanding that the officers may use technical aids during the surveillance, insofar as they are able to do so by the means of the Host State has obtained authorisation on the basis of the request referred to in Article 40 of the Convention implementing the Schengen Agreement. The Contracting Parties shall inform each other about the nature and use of technical observation aids. - The transboundary surveillance may also take place in airspace, maritime and waterways, subject to national law	Treaty of 08-06-2004 between the Kingdom of the Netherlands, the Kingdom of Belgium and the Grand Duchy of Luxembourg regarding cross-border police intervention http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2004060848&table_name=wet
What thresholds must be passed for the use of this tool?	So for observation without technical aid, there is no threshold (thus can be used for all criminal offences). For an observation with technical aid, the criminal offense has to be punishable with a correctional sentence of at least one year (see above).	Art. 47sexies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
What types of stakeholder are involved in the implementation of this tool?	- Public Prosecutor: The public prosecutor is responsible for permanent control over the application of the special investigation methods by the police services within his judicial district. - Federal Prosecutor: The public prosecutor informs the federal prosecutor of the special investigative methods used in his judicial district. If the application of the special investigation methods extends over several judicial districts or falls within the competence of the federal prosecutor, the competent public prosecutors and the federal prosecutor shall immediately inform each other and take all necessary measures to ensure the proper conduct of the proceedings to insure the operation. - Federal Police: For each decentralised judicial directorate, an officer is charged with permanent control over the special investigative methods in the district.	* Art. 47ter Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
Which LEAs can use this tool?	Special Investigation methods (observation, infiltration and use of informants) are carried out by the judicial directory of the Federal Police.	* Directive of 20-02-2002 regulating the division of tasks, cooperation, coordination and integration between the local and federal police in the tasks of judicial police http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=200202031&table_name=wet
What are the rules to be followed for the implementation of this tool?	There are four basic principles underlying the special investigation methods and techniques of the police: 1) Subsidiarity: This means that the methods are only to be employed, if the investigation, according to the facts, requires it and if the other means of investigation do not seem to be sufficient, which is decided a priori and in abstract by the magistrate who authorizes it. There is no requirement for the classic investigation methods to actually be tested - or that one must await the failure of the classic detection techniques before using a special method. 2) Proportionality: this implies that the used method should be proportional to the severity of the crime and it implies the chosen method should be proportionate to the goal. The limitation or breach of individual rights and freedoms can only be allowed in case of one serious breach of the legal order. Proportionality also means that before the action begins, there should be objective data that strongly suggest that the target individuals are committing criminal acts or are about to do so. So-called fishing expeditions or exploratory operations with use of undercover techniques are therefore excluded. 3) Non-provocation: When implementing a special investigation method, a police officer may not bring a suspect to commit other criminal offenses than those on which his intent was previously aimed. In case of violation, the criminal action is declared inadmissible with regard to these facts. 4) Prohibition to commit crimes: Crimes committed by police officers: The police officer charged with carrying out the special investigative methods is prohibited from committing criminal offenses in the context of his assignment. Police officers who, in the context of their assignment and with a view to its success or in order to ensure their own safety or that of other persons involved in the operation, remain free from punishment, commit strictly	- Art. 47quater Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel - Art. 47quinquies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel

Relevant items	Provisions	Sources used
	necessary criminal offenses, provided explicitly agreement of the public prosecutor. Those offenses must not be more serious than those for which the methods are used and must necessarily be proportionate to the aim pursued.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	The authorisation to observe is in writing and states: 1) The serious indications of the criminal offense that justify the observation, or, if the observation is part of the proactive investigation, the reasonable suspicion that it is or has already been committed but not yet at the uncovered offenses, and the special instructions relating to the elements described in this last provision, which justify the observation. 2) The reasons why the observation is indispensable to reveal the truth. 3) The name or, if not known, a description as accurate as possible of the person or persons being observed, as well as of the objects, places or events. 4) The manner in which the observation will be carried out, including the permission to use technical aids. In the latter case, the authorisation of the examining magistrate will state the address or the most accurate location of the home to which the observation relates. 5) The period during which the surveillance can be carried out and which may not be longer than three months from the date of the authorisation. 6) The name and capacity of the judicial police officer, who is in charge of carrying out the surveillance. At that time, the public prosecutor shall state in a separate written decision the crimes that can be committed by the police forces within the framework of the surveillance. This decision is kept in the file. In urgent cases, the authorisation for observation can be issued orally. The authorisation must be confirmed as soon as possible in the form. The public prosecutor can always change, supplement or extend his authorisation for observation in a motivated manner. He can revoke his authorisation at any time. He verifies with every amendment, addition or extension of his authorisation whether the conditions have been fulfilled. The public prosecutor is responsible for the enforcement of the authorisations of observation granted by the investigating judge in the context of a judicial investigation.	• Art. 47sexies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
What ongoing supervision is required for the use of this tool?	• The officer of the judicial police shall report accurately, completely and truthfully in writing to the public prosecutor on each stage in the execution of the observations he is in charge of. These confidential reports are sent directly to the Public Prosecutor, who keeps them in a separate and confidential file. He has sole access to this file, without prejudice to the right of inspection of the investigating judge and of the indictment chamber. The content of this file is covered by professional secrecy. • The authorisation to observe and the decisions to change, supplement or extend are attached to the confidential file. The officer of the judicial police draws up an official report of the different phases of the execution of the observation, but does not mention any elements that prevent the protection of the technical aids and the police investigation techniques used or jeopardize the safeguarding of security and the concealment of the identity of the informant and of the police officers in charge of conducting the surveillance. These elements are only included in the written report. An official report refers to the authorisation for observation. The public prosecutor confirms by written decision the existence of the authorisation to observe. • At least every three months, the Public Prosecutor sends all files in which he has applied the special investigation methods (observation, infiltration and civilian infiltration) and in which he has decided not to prosecute, to the Attorney General in order to enable them to verify the legality of the methods used. The Attorney General reports on this check. This report also deals with the application of the special investigative methods in the context of the execution of sentences or deprivation of liberty measures in its jurisdiction. The report is sent to the Board of Attorney General, which includes the global evaluation and the statistical data relating to these reports in its annual report. In his annual report, the federal prosecutor publishes the global evaluation and the statistical data of the files in which he has applied the special investigation methods (observation, infiltration and civilian infiltration) and in which he has decided not to prosecute. This report also deals with the application of the special investigative methods in the context of the execution of sentences or deprivation of liberty measures for federal criminal files. • The reports drawn up shall be added to the criminal file no later than after the observation has ended.	• Art. 47septies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel • Art. 47undecies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel

Relevant items	Provisions	Sources used
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	2016: 849 2017: 817 2018: 793	rapport annuel 2018 alpha-nl.pdf (om-mp.be)
Undercover / covert operations		
Relevant documents (legal and non-legal) that define the functioning of the tool	Code of Criminal Procedure dd. 17-11-1808, section III Special Investigation Methods, subsection 4 Infiltration (Infiltration = undercover / covert operations).	http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
How is the tool defined?	Infiltration within the meaning of this Code is the permanent contact by a police officer, referred to as an undercover officer, under a fictitious identity, with one or more persons, of whom there are serious indications that they have committed criminal offenses in the context of a criminal organisation, as referred to in Article 324bis of the Criminal Code, or commit or would commit crimes or offenses as referred to in Article 90ter, §§ 2 to 4 (list of criminal offenses).	Art. 47octies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
For what types of crime can the tool be used?	Infiltration can be used in the following cases: - Art. 324bis Criminal Code dd. 08-06-1867: By criminal organisation is meant any structured association of more than two persons that lasts over time, with the aim of committing by mutual agreement crimes and offenses punishable by imprisonment of three years or a more severe sentence, in order to obtain direct or indirect capital gains to gain. - Art. 90ter §2-§4 Code of Criminal Procedure dd. 17-11-1808: List of crimes with reference to Criminal Code dd. 08-06-1867.	- Criminal Code: http://www.ejustice.just.fgov.be/eli/wet/1867/06/08/1867060850/justel - Code of Criminal Procedure: http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
Does national law allow this tool to be used in cross-border cases?	No specific national regulations. Before a cross-border infiltration can be carried out, one must first request for assistance to the competent authorities of the requested State. This request for mutual assistance must therefore also be separately approved by the designated authorities of the requested country. That way, the countries in scope can establish an agreement in which the further specifications are included.	FOREIGN AFFAIRS, Second Additional Protocol to the European Convention on mutual legal assistance in criminal matters, 8 November 2001 http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2001110867&table_name=wet
What thresholds must be passed for the use of this tool?	Infiltration can thus only be used for crimes committed by a criminal organisation (art. 324bis Criminal Code dd. 08-06-1867) or for a limited list of crimes (art. 90ter §2-§4 Code of Criminal Procedure dd. 17-11-1808).	Art. 47octies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
What types of stakeholder are involved in the implementation of this tool?	- Public Prosecutor: The public prosecutor is responsible for permanent control over the application of the special investigation methods by the police services within his judicial district. - Federal Prosecutor: The public prosecutor informs the federal prosecutor of the special investigative methods used in his judicial district. If the application of the special investigation methods extends over several judicial districts or falls within the competence of the federal prosecutor, the competent public prosecutors and the federal prosecutor shall immediately inform each other and take all necessary measures to ensure the proper conduct of the proceedings to insure the operation. - Federal Police: For each decentralised judicial directorate, an officer is charged with permanent control over the special investigative methods in the district.	Art. 47ter Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
Which LEAs can use this tool?	Special Investigation methods (observation, infiltration and use of informants) are carried out by the judicial directory of the Federal Police.	* Directive of 20-02-2002 regulating the division of tasks, cooperation, coordination and integration between the local and federal police in the tasks of judicial police http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2002022031&table_name=wet
What are the rules to be followed for the implementation of this tool?	There are four basic principles underlying the special investigation methods and techniques of the police: 1) Subsidiarity: This means that the methods are only to be employed, if the investigation, according to the facts, requires it and if the other means of investigation do not seem to be sufficient, which is decided a priori and in abstract by the magistrate who authorizes it. There is no requirement for the classic investigation methods to actually be tested - or that one must await the failure of the classic detection techniques before using a special method. 2) Proportionality: this implies that the used method should be proportional to the severity of the crime and it implies the chosen method should be proportionate to the goal. The limitation or breach of individual rights and freedoms can only be allowed in case of one serious breach of the legal order. Proportionality also means that before the action begins, there should be objective data that strongly suggest that the target individuals are committing criminal acts or are about to do so. So-called fishing expeditions or exploratory operations with use of undercover techniques are therefore excluded. 3) Non-provocation: When implementing a special investigation method, a police officer may not bring a suspect to commit other criminal offenses than those on which his intent was	- Art. 47quater Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel - Art. 47quinquies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel

Relevant items	Provisions	Sources used
	previously aimed. In case of violation, the criminal action is declared inadmissible with regard to these facts. 4) Prohibition to commit crimes: Crimes committed by police officers: The police officer charged with carrying out the special investigative methods is prohibited from committing criminal offenses in the context of his assignment. Police officers who, in the context of their assignment and with a view to its success or in order to ensure their own safety or that of other persons involved in the operation, remain free from punishment, commit strictly necessary criminal offenses, provided explicitly agreement of the public prosecutor. Those offenses must not be more serious than those for which the methods are used and must necessarily be proportionate to the aim pursued.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	The public prosecutor can authorize an infiltration in the context of the criminal investigation if the investigation so requires and the other means of investigation do not appear to be sufficient to reveal the truth. He can authorize the police service, within the legal framework of an infiltration and with due observance of its purpose, to use certain police investigation techniques. The public prosecutor can also, if there is reason to do so, grant permission to take the necessary measures to safeguard the security and the physical, psychological and moral integrity of the undercover officer. The authorisation for infiltration is in writing and states: 1) The serious indications of the criminal offense that justify the infiltration or, if the infiltration is part of the proactive investigation the reasonable suspicion that it has been committed or has already been committed but has not yet been discovered offenses committed, and the special instructions relating to the elements described in this last provision, justifying the infiltration. 2) The reasons why the infiltration is indispensable to reveal the truth. 3) If known, the name or otherwise a description as accurate as possible of the person or persons referred to. 4) The manner in which the infiltration will be carried out, including the permission to briefly call on the expertise of a citizen and the admission of police investigation techniques to use. 5) The period during which the infiltration can be carried out and which may not exceed three months from the date of the authorisation. 6) The name and capacity of the judicial police officer who is in charge of carrying out the infiltration. At that time, the public prosecutor will state in a separate written decision the crimes that can be committed by the police forces, in the context of the infiltration. The public prosecutor can always change, supplement or extend his authorisation to infiltrate in a motivated manner. He can revoke his authorisation at any time. He verifies with every amendment, addition or extension of his authorisation whether the conditions stipulated have been fulfilled. The public prosecutor is responsible for the enforcement of the authorisations for infiltration granted by the investigating judge in the context of a judicial investigation.	• Art. 47octies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
What ongoing supervision is required for the use of this tool?	The officer of the judicial police will report accurately, completely and truthfully in writing to the Public Prosecutor on each stage in the execution of the infiltrations under his control. These confidential reports are sent directly to the Public Prosecutor, who keeps them in a separate and confidential file. He has sole access to this file, without prejudice to the right of inspection of the investigating judge and of the indictment chamber. The content of this file is covered by professional secrecy. The authorisation to infiltrate and the decisions to amend, supplement or extend are attached to the confidential file. The officer of the judicial police draws up an official report of the different phases of the execution of the infiltration, but does not mention any elements that prevent the protection of the technical aids and the police investigation techniques used. whether the safeguarding of the security and the protection of the identity of the informant, the police officers charged with carrying out the infiltration can jeopardize. These elements are only included in the written report. An official report refers to the authorisation to infiltrate. The public prosecutor confirms by written decision the existence of the authorisation for infiltration granted by him. The reports drawn up shall be added to the criminal file no later than after the infiltration has been completed. At least every three months, the Public Prosecutor sends all files in which he has applied the special investigation methods (observation, infiltration and civilian infiltration) and in which he has decided not to prosecute, to the Attorney General in order to enable them to verify the legality of the methods used. The Attorney General reports on this check. This report also deals with the application of the special investigative methods in the context of the execution of	• Art. 47novies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel • Art. 47undecies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel

Relevant items	Provisions	Sources used
	sentences or deprivation of liberty measures in its jurisdiction. The report is sent to the Board of Attorney General, which includes the global evaluation and the statistical data relating to these reports in its annual report. In his annual report, the federal prosecutor publishes the global evaluation and the statistical data of the files in which he has applied the special investigation methods (observation, infiltration and civilian infiltration) and in which he has decided not to prosecute. This report also deals with the application of the special investigative methods in the context of the execution of sentences or deprivation of liberty measures for federal criminal files.	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	2016: 42 2017: 45 2018: 48	rapport annuel 2018 alpha-nl.pdf (om-mp.be)
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	Code of Criminal Procedure dd. 17-11-1808, section III Special Investigation Methods, subsection 5 Use of informants	http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
Specific range of application of the tool	National legislation only has one definition of an informant (see below)	Art. 47decies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
How is the tool defined?	Use of informants within the meaning of this Code is the maintenance of regular contacts by a police officer with a person, called an informant, who is suspected of having close ties with one or more persons, of whom there are serious indications that they are committing or would be committing criminal offenses , and who provides the police officer with information and data about this, whether or not requested. This police officer is called a liaison officer.	Art. 47decies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
For what types of crime can the tool be used?	No Limitations.	Art. 102-111decies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
Does national law allow this tool to be used in cross-border cases?	Nothing defined.	
What thresholds must be passed for the use of this tool?	No Limitations.	
What types of stakeholder are involved in the implementation of this tool?	* Within the directorate of officers, which is part of the general directorate of the judicial police of the federal police, an officer in charge of the national management of the informant work within the integrated police service is structured on two levels. This officer, referred to as the national informant manager, may be assisted in the performance of his duties by one or more officers of the judicial police. He supervises compliance with the regulations applicable in or pursuant to this article. The National Informant Administrator acts under the authority of the federal prosecutor. * Within each decentralized judicial directorate, an officer, called the local informant manager, is charged with the district management of the informant work within the devolved judicial (management) and local police forces of the district. To this end, he exercises permanent control over the reliability of the informants and supervises compliance with the regulations applicable in or pursuant to this article and the proper functioning of the liaison officers. The local informant manager acts under the authority of the public prosecutor. * In each local police force, within which informant work is carried out, an officer is appointed to assist the local informant manager in his assignment.	Art. 47decies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
Which LEAs can use this tool?	* Federal Police * Local Police	Art. 47decies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
What are the rules to be followed for the implementation of this tool?	The use of informants is not linked to any subsidiarity or proportionality requirement. The Government reiterated with regard to the proportionality requirement is its position that, if per hypothesis the use of informants would be limited to certain offenses, it would not make sense to exclude the information that could be provided by the informant about other crimes of the field of application of the law. One would then lack information that can lead to the occurrence of one crime or its elimination	Art. 47quater Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel Art. 47quinquies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	On the recommendation of the Minister of Justice and after advice from the Board of Attorney General and the Federal Prosecutor, the King determines the operating rules of the national and local informant administrators and of the liaison officers, with due observance of a permanent	Art. 47decies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel

Relevant items	Provisions	Sources used
	control over the reliability of the informants, the protection of the identity of the informants and the safeguarding of the physical, psychological and moral integrity of the liaison officers.	
What ongoing supervision is required for the use of this tool?	The local informant manager shall at his request and at least quarterly report to the public prosecutor on the informant activities within the devolved judicial management and the local police forces of the district. The National Informant Administrator submits to the Federal Prosecutor at his request and at least quarterly general report on the informant activities within the integrated police service structured at two levels. If the informant reveals serious indications about committed or yet to be committed criminal offenses, the local informant manager will immediately and in writing accurately and accurately report this to the public prosecutor and report truthfully. The public prosecutor can also, if there are grounds to do so, prohibit the local informant manager by written decision to continue working on certain information provided by an informant. The public prosecutor keeps these confidential reports in a separate file. He is the only person who has access to this file, without prejudice to the right of inspection of the investigating judge. The content of this file is covered by professional secrecy. He decides whether, depending on the importance of the information provided and taking into account the safety of the informant, an official report is drawn up. If this official report relates to an ongoing criminal investigation or judicial investigation, the public prosecutor is responsible for attaching it to this criminal file.	Art. 47decies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Pseudo purchase, trust purchase and test purchase, Pseudo sale and trust sale, Front store		
Relevant documents (legal and non-legal) that define the functioning of the tool	Royal decree of 09-04-2003 regarding police investigation techniques.	http://www.ejustice.just.fgov.be/eli/besluit/2003/04/09/2003009348/justel
How is the tool defined?	- Pseudo purchase (art. 3): Pseudo-purchase is the technique, used by a police force, whereby a person is presented or presented as a potential buyer of a service or of a good, and of which this person wishes to transfer ownership for his own account or for the account of another person. - Trust purchase (art. 3): The trust purchase is the technique, used by a police force, whereby a person is presented or presented as a potential purchaser of a service or of a good, and of which that person wishes to transfer ownership for his own account or for the account of another, and whereby ownership is effectively transferred, in order to gain the trust of the seller and gather additional information. - Test purchase (art. 3): The test purchase is the technique, used by a police force, whereby a person is presented or presented as a potential purchaser of a service or of a good, and of which this person wishes to transfer ownership for his own account or for the account of another, and whereby the ownership is effectively transferred, in order to verify the claims of the seller and the veracity of the good offered. - Pseudo sale (art. 4): Pseudo-sale is the technique, used by a police force, whereby one presents or is presented to a person as a potential seller of a service or good. - Trust sale (art. 4): Trust sale is the technique, employed by a police force, whereby one presents or is presented to a person as a potential seller of a service or good, and whereby ownership is effectively transferred in order to gain the buyer's trust and collect additional information. - Front store (art. 7): The front store is the technique whereby one or more companies are actually set up or operated by or on behalf of the police services, possibly on the basis of fictitious data, by means of which support in the form of goods or services can be offered to the criminal environment.	Royal decree of 09-04-2003 regarding police investigation techniques http://www.ejustice.just.fgov.be/eli/besluit/2003/04/09/2003009348/justel
For what types of crime can the tool be used?	Infiltration can be used in the following cases: - Art. 324bis Criminal Code dd. 08-06-1867: By criminal organisation is meant any structured association of more than two persons that lasts over time, with the aim of committing by mutual agreement crimes and offenses punishable by imprisonment of three years or a more severe sentence, in order to obtain direct or indirect capital gains. - Art. 90ter §2-§4 Code of Criminal Procedure dd. 17-11-1808: List of crimes with reference to Criminal Code dd. 08-06-1867.	- Criminal Code: http://www.ejustice.just.fgov.be/eli/wet/1867/06/08/1867060850/justel - Code of Criminal Procedure: http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
Does national law allow this tool to be used in cross-border cases?	Nothing defined.	

Relevant items	Provisions	Sources used
What thresholds must be passed for the use of this tool?	Infiltration can thus only be used for crimes committed by a criminal organisation (art. 324bis Criminal Code dd. 08-06-1867) or for a limited list of crimes (art. 90ter §2-§4 Code of Criminal Procedure dd. 17-11-1808).	Art. 47octies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
What types of stakeholder are involved in the implementation of this tool?	- Public Prosecutor: The public prosecutor is responsible for permanent control over the application of the special investigation methods by the police services within his judicial district. - Federal Prosecutor: The public prosecutor informs the federal prosecutor of the special investigative methods used in his judicial district. If the application of the special investigation methods extends over several judicial districts or falls within the competence of the federal prosecutor, the competent public prosecutors and the federal prosecutor shall immediately inform each other and take all necessary measures to ensure the proper conduct of the proceedings to insure the operation. - Federal Police: For each decentralised judicial directorate, an officer is charged with permanent control over the special investigative methods in the district.	Art. 47ter Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
Which LEAs can use this tool?	Special Investigation methods (observation, infiltration and use of informants) are carried out by the judicial directory of the Federal Police.	Directive of 20-02-2002 regulating the division of tasks, cooperation, coordination and integration between the local and federal police in the tasks of judicial police http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=200202031&table_name=wet
What are the rules to be followed for the implementation of this tool?	There are four basic principles underlying the special investigation methods and techniques of the police: 1) Subsidiarity: This means that the methods are only to be employed, if the investigation, according to the facts, requires it and if the other means of investigation do not seem to be sufficient, which is decided a priori and in abstract by the magistrate who authorizes it. There is no requirement for the classic investigation methods to actually be tested - or that one must await the failure of the classic detection techniques before using a special method. 2) Proportionality: this implies that the used method should be proportional to the severity of the crime and it implies the chosen method should be proportionate to the goal. The limitation or breach of individual rights and freedoms can only be allowed in case of one serious breach of the legal order. Proportionality also means that before the action begins, there should be objective data that strongly suggest that the target individuals are committing criminal acts or are about to do so. So-called fishing expeditions or exploratory operations with use of undercover techniques are therefore excluded. 3) Non-provocation: When implementing a special investigation method, a police officer may not bring a suspect to commit other criminal offenses than those on which his intent was previously aimed. In case of violation, the criminal action is declared inadmissible with regard to these facts. 4) Prohibition to commit crimes: Crimes committed by police officers: The police officer charged with carrying out the special investigative methods is prohibited from committing criminal offenses in the context of his assignment. Police officers who, in the context of their assignment and with a view to its success or in order to ensure their own safety or that of other persons involved in the operation, remain free from punishment, commit strictly necessary criminal offenses, provided explicitly agreement of the public prosecutor. Those offenses must not be more serious than those for which the methods are used and must necessarily be proportionate to the aim pursued.	- Art. 47quater Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel - Art. 47quinquies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool?(e.g. senior police officer, prosecutor, judge, other)	The public prosecutor can authorize an infiltration in the context of the criminal investigation if the investigation so requires and the other means of investigation do not appear to be sufficient to reveal the truth. He can authorize the police service, within the legal framework of an infiltration and with due observance of its purpose, to use certain police investigation techniques. The public prosecutor can also, if there is reason to do so, grant permission to take the necessary measures to safeguard the security and the physical, psychological and moral integrity of the undercover officer. The authorisation for infiltration is in writing and states: 1) The serious indications of the criminal offense that justify the infiltration or, if the infiltration is part of the proactive investigation the reasonable suspicion that it has been committed or has already been committed but has not yet been discovered offenses committed, and the special instructions relating to the elements described in this last provision, justifying the infiltration. 2) The reasons why the infiltration is indispensable to reveal the truth. 3) If known, the name or otherwise a description as accurate as possible of the person or persons referred to.	- Art. 47octies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel - Art. 9 Royal decree of 09-04-2003 regarding police investigation techniques

Relevant items	Provisions	Sources used
	4) The manner in which the infiltration will be carried out, including the permission to briefly call on the expertise of a citizen and the admission of police investigation techniques to use. 5) The period during which the infiltration can be carried out and which may not exceed three months from the date of the authorisation. 6) The name and capacity of the judicial police officer who is in charge of carrying out the infiltration. At that time, the public prosecutor will state in a separate written decision the crimes that can be committed by the police forces, in the context of the infiltration. The public prosecutor can always change, supplement or extend his authorisation to infiltrate in a motivated manner. He can revoke his authorisation at any time. He verifies with every amendment, addition or extension of his authorisation whether the conditions stipulated have been fulfilled. The public prosecutor is responsible for the enforcement of the authorisations for infiltration granted by the investigating judge in the context of a judicial investigation. The police investigation techniques of the front store require the prior written agreement of the federal prosecutor. In case of controlled delivery of persons and controlled onward delivery, this agreement can be provided verbally in urgent circumstances. The agreement will be confirmed in writing as soon as possible.	
What ongoing supervision is required for the use of this tool?	The officer of the judicial police will report accurately, completely and truthfully in writing to the Public Prosecutor on each stage in the execution of the infiltrations under his control. These confidential reports are sent directly to the Public Prosecutor, who keeps them in a separate and confidential file. He has sole access to this file, without prejudice to the right of inspection of the investigating judge and of the indictment chamber. The content of this file is covered by professional secrecy. The authorisation to infiltrate and the decisions to amend, supplement or extend are attached to the confidential file. The officer of the judicial police draws up an official report of the different phases of the execution of the infiltration, but does not mention any elements that prevent the protection of the technical aids and the police investigation techniques used whether the safeguarding of the security and the protection of the identity of the informant, the police officers charged with carrying out the infiltration can jeopardize. These elements are only included in the written report. An official report refers to the authorisation to infiltrate. The public prosecutor confirms by written decision the existence of the authorisation for infiltration granted by him. The reports drawn up shall be added to the criminal file no later than after the infiltration has been completed. At least every three months, the Public Prosecutor sends all files in which he has applied the special investigation methods (observation, infiltration and civilian infiltration) and in which he has decided not to prosecute, to the Attorney General in order to enable them to verify the legality of the methods used. The Attorney General reports on this check. This report also deals with the application of the special investigative methods in the context of the execution of sentences or deprivation of liberty measures in its jurisdiction. The report is sent to the Board of Attorney General, which includes the global evaluation and the statistical data relating to these reports in its annual report. In his annual report, the federal prosecutor publishes the global evaluation and the statistical data of the files in which he has applied the special investigation methods (observation, infiltration and civilian infiltration) and in which he has decided not to prosecute. This report also deals with the application of the special investigative methods in the context of the execution of sentences or deprivation of liberty measures for federal criminal files.	- Art. 47novies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel - Art. 47undecies Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	- Pseudo purchase, trust purchase and test purchase: N/A - Pseudo sale and trust sale: N/A - Front store: 3 in 2016, 7 in 2017 and 3 in 2018	rapport annuel 2018 alpha-nl.pdf (om-mp.be)
Civilian infiltration		
Relevant documents (legal and non-legal) that define the functioning of the tool	Code of Criminal Procedure dd. 17-11-1808, section III Special Investigation Methods, subsection 4bis Civilian infiltration.	http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
How is the tool defined?	Civilian infiltration within the meaning of this Code is a permanent and controlled contact by an adult person who is not a police officer, called a civilian infiltrator, if necessary under a fictitious identity, with one or more persons with regard to whom there are serious indications that they are one of the commit or would commit criminal offenses. The civilian is not necessarily involved in the criminal offenses.	Art. 47novies/1 Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel

Relevant items	Provisions	Sources used
For what types of crime can the tool be used?	Limited list of criminal offenses (art. 90ter, §2 - §4) when they are committed by a criminal organisation (art. 324bis Criminal Code) and terrorist crimes (book 2, title Iter Criminal Code).	Art. 47novies/1 Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
Does national law allow this tool to be used in cross-border cases?	Nothing defined.	
What thresholds must be passed for the use of this tool?	The tool can thus only be used for a limited list of criminal offences (when they are committed in the context of a criminal organisation) and for terrorist crimes.	Art. 47novies/1 Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
What types of stakeholder are involved in the implementation of this tool?	- The public prosecutor may, in the context of the criminal investigation, authorize a civilian infiltration if the investigation so requires and if the other means of the investigation, do not appear to be sufficient to reveal the truth. The authorisation or extension of the civil infiltration authorisation by the public prosecutor or by the investigating judge requires the prior agreement of the federal prosecutor. If this agreement was given orally, it will be confirmed in writing afterwards, as soon as possible. The agreement is kept in the confidential file. The public prosecutor can, within the legal framework of a civilian infiltration and with due observance of its purpose, authorize the police service, to carry out the police investigation technique to have the civilian infiltrator used under the supervision of the counselling officer. The public prosecutor can, if justified, grant permission to take the necessary measures to safeguard the safety and the physical, psychological and moral integrity of the civilian infiltrator. This permission is kept in the confidential file. - Police officers of the directorate of the special forces of the federal police who have received special training for this purpose, called escort officers, accompany the civilian infiltrator with a view to the proper performance of his task. Police officers from the Directorate of Special Forces of the Federal Police, called control officers, ensure the safeguarding of the security and physical, psychological and moral integrity of the civilian infiltrator, as well as the fulfilment of the obligations of the civilian infiltrator. A police officer cannot be simultaneously escort and control officer of the same civilian infiltrator.	Art. 47novies/1 Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
Which LEAs can use this tool?	Special Investigation methods (observation, infiltration and use of informants) are carried out by the judicial directory of the Federal Police.	Directive of 20-02-2002 regulating the division of tasks, cooperation, coordination and integration between the local and federal police in the tasks of judicial police http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=200202031&table_name=wet
What are the rules to be followed for the implementation of this tool?	The civilian infiltrator, the escort and control officers, are prohibited from committing criminal offenses in the context of the civil infiltrator's mission. The civilian infiltrator and the escort and control officers who, in the context of the civilian infiltrator's mission and with a view to its success or to ensure their own safety or that of other persons involved in the operation, remain free from punishment if they commit criminal offenses, with the explicit prior agreement of the public prosecutor. Those offenses may not be more serious than those for which the civilian infiltration is used, must necessarily be proportionate to the aim pursued and must not prejudice the physical integrity of persons. The magistrate, with due observance of this Code, shall remain free from punishment, authorizing a civilian infiltrator, escort and control officers and persons who do not belong to the police services but whose expertise is called upon to commit criminal offenses in connection with the implementation of civilian infiltration. The officer of the judicial police reports in writing to the public prosecutor the crimes that the civilian infiltrator and the escort and control officers may have to commit. . The civilian infiltrator immediately communicates his conduct and observations to the escort officers, who in turn report this to the officer of the judicial police. The latter notifies the public prosecutor.	Art. 47novies/1 Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool?(e.g. senior police officer, prosecutor, judge, other)	The authorisation for civilian infiltration is in writing and states: 1) The serious indications of the criminal offenses that justify the civilian infiltration or, if the civilian infiltration is part of the proactive investigation, the reasonable suspicion of a criminal offense to be committed or already committed but not yet discovered facts, and special indications with regard to the elements described in this last provision, which justify civilian infiltration. 2) The reasons why civilian infiltration is indispensable to reveal the truth, and in particular the reasons why the infiltration does not seem sufficient to reveal the truth. 3) If known, the name or otherwise a description as accurate as possible of the persons in respect of whom there are serious indications that they commit or would commit one of the offenses on condition that they are or would be committed within the framework of a criminal organisation, or one of the terrorist crimes. 4) The manner in which civilian infiltration will be carried out, including the permission to use police investigation techniques.	Art. 47novies/1 Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel

Relevant items	Provisions	Sources used
	5) The period during which the civilian infiltration can be carried out, which may not be longer than three months from the date of the authorisation. 6) The name and capacity of the officer of the judicial police, who is in charge of carrying out the civilian infiltration. 7) The identity of the citizen infiltrator in the form of a code. 8) The agreement of the federal prosecutor to authorize or extend civilian infiltration. If necessary, the public prosecutor shall state in a separate written decision the crimes that can be committed by the civilian infiltrator, the escort and control officers in the context of civilian infiltration. This decision is kept in the file. In urgent cases, the authorisation for civilian infiltration can be issued orally. The authorisation will be confirmed as soon as possible in the form. The public prosecutor can always amend, supplement or extend his authorisation for civilian infiltration in a reasoned manner. He can revoke his authorisation at any time. He verifies with every change, addition or extension of his authorisation whether the conditions stipulated have been fulfilled. The public prosecutor is responsible for the enforcement of the authorisations for civilian infiltration granted by the investigating judge in the context of a judicial investigation. If necessary, the public prosecutor shall state in a separate written decision the crimes that can be committed by the civilian infiltrator, escort and control officers.	
What ongoing supervision is required for the use of this tool?	The officer of the judicial police will report accurately, completely and truthfully in writing to the public prosecutor on each phase in the execution of the civilian infiltrations under his control. These confidential reports are sent directly to the Public Prosecutor, who keeps them in a separate and confidential file. He has sole access to this file, without prejudice to the right of inspection of the investigating judge and of the indictment chamber. The content of this file is covered by professional secrecy. The authorisation for civilian infiltration and the decisions to amend, supplement or extend are attached to the confidential file. The officer of the judicial police draws up an official report of the different phases of the execution of the civilian infiltration, but does not mention any elements that prevent the protection of the technical aids and police investigation techniques or the safeguarding of security and the protection of the identity of the informant, the civilian infiltrator, the police officers in charge of the surveillance, the infiltration and the civilian infiltration and of the persons who do not belong to the police services but on whose expertise is called upon. These elements are only included in the written report. An official report refers to the authorisation for civilian infiltration. The public prosecutor confirms by written decision the existence of the authorisation for civilian infiltration, of the risk analysis and the age of majority of the civilian infiltrator. The reports drawn up and the decision shall be added to the criminal file no later than after the end of the civilian infiltration, if necessary of the infiltration. Evidence obtained as a result of the application of civilian infiltration may only be taken into account as evidence on condition that it is sufficiently supported by other types of evidence. The control officers shall provide the director of judicial police operations of the federal police and the public prosecutor with an accurate, complete and truthful written report on public safety, the safety of the civilian infiltrator, the physical, psychological and moral integrity of the citizen infiltrator and the fulfilment of the obligations by the citizen infiltrator, who keeps them in the confidential file.	Art. 47novies/3 Code of Criminal Procedure http://www.ejustice.just.fgov.be/eli/wet/1808/11/17/1808111701/justel
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	

Source: Author's own elaboration

Bulgaria

Table 20 – Overview of national rules on investigative tools – Bulgaria

Relevant items	Provisions	Sources used
Controlled Delivery		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Procedure code Law on Special Intelligence means	- Law on Special Intelligence means - Criminal procedure code
How is the tool defined?	The import, export, transfer or transit through the territory of the Republic of Bulgaria by the controlled person, which is under constant surveillance, of a thing/goods - subject of a crime, to reveal the participants in cross-border crime.	

Relevant items	Provisions	Sources used
For what types of crime can the tool be used?	* According to art. 3 of the LSIM the Special intelligence tools (controlled delivery and all others) shall be used when necessary to prevent and detect serious intentional crimes under Chapter One, Chapter Two, Sections I, II, IV, V, VIII and IX, Chapter Three, Section III, Chapter Five, Sections I, VII, Chapter Six, Sections II-IV, Chapter Eight, Chapter Eight "a", Chapter Nine "a", Chapter Eleven, Sections I - IV, Chapter Twelve, Chapter Thirteen, and Chapter Fourteen, as well as for crimes under Art. 219, para. 4, proposal two, art. 220, para. 2, Art. 253, Art. 308, para. 2, 3, and 5, sentence two, art. 320, para. 2, Art. 321, Art. 321a, art. 356k and Art. 393 of the special part of the Criminal Code, when the necessary data cannot be collected in any other way or their collection is associated with exceptional difficulties. * According to art 3, some of these SOC are as follows: CRIMES AGAINST THE REPUBLIC, Murder, Injury, Kidnapping and unlawful deprivation of liberty, Coercion, Debauchery, Human Trafficking, Crimes against the political rights of citizens, Theft, Drugs, etc.	
Does national law allow this tool to be used in cross-border cases?	Yes, the tool can be used both for national criminal investigation and for cross border criminal investigations	
What thresholds must be passed for the use of this tool?	* According to the Penal Code the punishments depend on the crime and could be from a financial fine to a life sentence (with parole and without parole). *For the most serious crimes, which threaten the foundations of the republic, as well as for other especially dangerous crimes (including those the controlled delivery tool applied for), the sanction is life imprisonment without parole. * The penalties are stricter when the monetary equivalent of the subject of the crime is "large amounts" or "especially large amounts". * When determining the qualifiers "large amounts" and "especially large amounts" for different types of crimes, unless otherwise specified in the law, the criteria is the monetary equivalent of the subject of the crime, which exceeds 70, respectively 140 times the minimum working salary. * However, when the crime is related to taxes (tax evasion), there are other definitions for large and especially large amounts. Taxes in large amounts "are those that exceed three thousand leva (BGN 3000), and" taxes in especially large amounts "are those that exceed twelve thousand leva (BGN 12 000).	
What types of stakeholder are involved in the implementation of this tool?	LEAs and Judicial Authorities	
Which LEAs can use this tool?	1. National Police: General Directorate "National Police", General Directorate "Fight against Organized Crime", General Directorate "Border Police", Directorate "Internal Security", regional directorates of the Ministry of Interior 2. Financial Security Unit (State Agency National Security): specialized directorates (except for "Technical Operations"), the territorial directorates and the independent territorial departments of the State Agency for National Security; 3. The Prosecutor's Office 4. The National Investigative Service 5. The Military Intelligence and Military Police services part of the Minister of Defense	
What are the rules to be followed for the implementation of this tool?	Although controlled delivery is introduced in the Criminal Procedure Code and defined in the Law on the Special Intelligence Means together with other special investigative tools, it still lacks a detailed and systematic regulation and is not used sufficiently. Since this technique is applied to prove the cross-border crimes where illicit subject of the delivery moves in different countries, it requires a mechanism of interaction between their competent authorities. Such a mechanism is set up within the EU - in each case permission is required for controlled delivery in the territory of the requested State of its competent authority. It is generally easier when the subject of the controlled delivery is carried out in Member States. In other cases, difficulties may arise because of the need for bilateral cooperation mechanisms. Apart from the general rules for the preparation of physical means of proof, the Criminal Procedure Code does not make any express provisions on the way of preparing means of proof using the rest of the operational techniques. These can make the use of this tool for proving criminal activities difficult.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	According to art. 57 of the Constitution of the Republic of Bulgaria (1) The fundamental civil rights are inalienable.and (2) Abuse of rights shall not be allowed. The main principle for equality is set up in the Constitution of the Republic of Bulgaria and the Criminal Procedure Code. According to art. 11 of the Criminal Procedure Code, all citizens involved in criminal proceedings has equal rights. No restrictions on rights or privileges based on race, nationality, ethnicity, gender, origin, religion, education, beliefs, political affiliation, personal and social status, or property status are permitted. (2) The court, the prosecutor and the investigating bodies shall apply the laws accurately and equally to all citizens.	• Criminal Procedure Code • CONSTITUTION OF THE REPUBLIC OF BULGARIA

Relevant items	Provisions	Sources used
	Other principles set up by the criminal laws are: right to defense, presumption of innocence, disclosure of objective truth, adversarial proceedings, equal rights of the parties, Independence of the bodies of criminal proceedings	
What authorisation is needed for the use of this tool?	Depending on the crime and the subject an authorisation request for the use of this tool must be submitted to: 1. the chairmen of the Sofia City Court, 2. the respective district or military courts, 3. the specialized criminal court or to a deputy chairman authorized by them, who within 48 hours give written permission for the use of special intelligence means or refuse their use. In the cases of imminent danger of committing a serious intentional crime or in case of threat to the national security the special intelligence means may be used without permission of the body of art. 15 on the basis of an order of the Chairman of the State Agency "Technical Operations", the Chairman of the State Agency "National Security" or the Secretary General of the Ministry of Interior.	• Law on Special Intelligence means • Criminal procedure code
What ongoing supervision is required for the use of this tool?	Control over the application and use of special intelligence means is exercised by: 1. the Chairman of the State Agency "Technical Operations", when the special intelligence means are applied and used by the agency; 2. the Chairman of the State Agency "National Security", when the special intelligence means are applied and used by the structures of the State Agency "National Security"; 3. the Minister of Interior, when special intelligence means are used under Art. 10c ZMVR. The National Bureau for the Control of Special Intelligence Measures is an independent state body that monitors the procedures for authorization, implementation and use of special intelligence means, storage and destruction of information obtained through special intelligence means. as well as for the protection of the rights and freedoms of citizens against the illegal use of special intelligence means.	
Is there any national case law relating to the use of this tool in cross-border crime cases?	There is some national case law (in Bulgarian), related to the application of this tool. Most of the crimes are related to cross-border drug trafficking. This tool is used very often along with other Special Intelligence tools like surveillance, eavesdropping, and tracking. Attached is a court decision (RESOLUTION № 280, Sofia, February 27, 2017 of The Supreme Court of Cassation of the Republic of Bulgaria). It is about the cross-boarder traffic of drugs (cocaine). The defendants are Bulgarian citizens, who were justified. A controlled delivery tool was applied during the investigation, however a lot of mistakes were performed by the police officers, as a result, the defendants claimed that the authority (police) did not collect the evidence according to the law and fundamental rights have been violated.	National case law
Data available on the number of times this tool has been used for SOC cases	According to the the last available Report of The National Bureau for the Control of Special Intelligence Measures (page 18). The use of controlled delivery tool was requested and approved as follows: *in 2019 - 2 times *in 2018 - 7 times *in 2017 - 38 times	Annual Report of The National Bureau for the Control of Special Intelligence Measures link .
Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	According to the Criminal Procedure Code this tool is not available (in the meaning urgent and direct pursuit of a criminal suspect by law enforcement officers). Close to this tool is Tracking (following) of the persons. According to art. 172 of the Criminal Procedure Code and art. 2 of the Law on Special Intelligence means the investigative tools are as follows: surveillance, eavesdropping, tracking, infiltration, marking, recording and verification of correspondence and computer information, controlled delivery, confidential transaction and investigation through an undercover officer	• Criminal Procedure Code • LAW ON THE PROTECTION OF PERSONS THREATENED IN CONNECTION WITH CRIMINAL PROCEEDINGS
How is the tool defined?	N/A	
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross-border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	N/A	

Relevant items	Provisions	Sources used
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Procedure Code LAW ON THE PROTECTION OF PERSONS THREATENED IN CONNECTION WITH CRIMINAL PROCEEDINGS	
How is the tool defined?	I. First type of protection: The prosecutor or the court, at the request of the witness or with their consent, shall take measures for their immediate protection when there are sufficient grounds to believe that the testimony has given rise or may give rise to a real danger to the life or health of the witness, his ascendants, descendants, brothers, sisters, spouse or persons with whom he has a particularly close relationship. Witness protection is temporary and is carried out through: - providing personal physical protection from: - the bodies of the Ministry of Interior; - the employees of the Protection Bureau at the Chief Prosecutor - keeping his identity secret. The relevant bodies of the pre-trial proceedings and the court have direct access to the protected witness, and the defense counsel and the trustee (if pointed) 2. Second type of protection or so called Special protection Within thirty days from the taking of a measure under art 123, para. 2 of the Criminal Procedure Code, the prosecutor or the court may propose the inclusion of the witness or his ascendants, descendants, brothers, sisters, spouse or persons with whom he is in a particularly close relationship, in the protection program under the LAW ON THE PROTECTION OF PERSONS THREATENED IN CONNECTION WITH CRIMINAL PROCEEDINGS (so called Special Protection) Special protection may also include activities to provide social, medical, psychological, legal and financial assistance to support the integration of the person into the new environment. The special protection includes the following measures: - personal physical security; - protection of the property; - accommodation in a safe place; - accommodation in another place for serving the punishment. (2) The protection program shall include the following measures: - change of the place of residence in the country; - change of the place of work; - change of the nursery or institution in the pre-school, school and higher education; - accommodation in another place for serving the punishment; - relocation in another state under the conditions of art. 27, para. 1, items 1 and 2.	- Criminal Procedure Code - LAW ON THE PROTECTION OF PERSONS THREATENED IN CONNECTION WITH CRIMINAL PROCEEDINGS
For what types of crime can the tool be used?	there are no limitations. The protection does not depend on the crime, depends on the grounds. Art. 123, para 2 "... there are sufficient grounds to believe that the testimony has given rise or may give rise to a real danger to the life or health of the witness..."	Law on Special Intelligence means Criminal procedure code
Does national law allow this tool to be used in cross-border cases?	Yes, the tool can be used both for national criminal investigation and for cross border criminal investigations	
What thresholds must be passed for the use of this tool?	* According to the Penal Code the punishments depend on the crime and could be from a financial fine to a life sentence (with parole and without parole).	art. 37 of the Penal Code

Relevant items	Provisions	Sources used
	*For the most serious crimes, which threaten the foundations of the republic, as well as for other especially dangerous crimes (including those the controlled delivery tool applied for), the sanction is life imprisonment without parole. * The penalties are stricter when the monetary equivalent of the subject of the crime is "large amounts" or "especially large amounts". * When determining the qualifiers "large amounts" and "especially large amounts" for different types of crimes, unless otherwise specified in the law, the criteria is the monetary equivalent of the subject of the crime, which exceeds 70, respectively 140 times the minimum working salary. * However when the crime is related to taxes (tax evasion), there are other definitions for large and especially large amounts. Taxes in large amounts "are those that exceed three thousand levs (BGN 3000), and" taxes in especially large amounts "are those that exceed twelve thousand levs (BGN 12 000).	
What types of stakeholder are involved in the implementation of this tool?	The prosecutor or the court	- art. 123, para 2 of the Criminal Procedure Code - Law on Special Intelligence means
Which LEAs can use this tool?	1. First type of protection: The witness can ask for a protection or can submit consent for a protection (usually the court or the prosecutor ask the witness whether there is a need for protection) 2. Special protection is provided by the Office of Defense under the Chief Prosecutor Provision of special protection is carried out at the proposal of the district prosecutor, and in court proceedings - to the court, through the Bureau of Protection, to the chief prosecutor. (2) The proposal for granting protection shall be made ex officio or at the request of: 1. the endangered person; 2. the investigative body; 3. the supervising prosecutor; 4. the chief of the place for deprivation of liberty - for convicted persons. An explicit written consent of the witness is also required.	art. 13, para 1 of the Law on Special Intelligence means
What are the rules to be followed for the implementation of this tool?	The steps depends on the different protection required. See above the requirements for the two type of protections.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	According to art. 57 of the Constitution of the Republic of Bulgaria (1) The fundamental civil rights are inalienable.and (2) Abuse of rights shall not be allowed. The main principle for equality is set up in the Constitution of the Republic of Bulgaria and the Criminal Procedure Code. According to art. 11 of the Criminal Procedure Code, all citizens involved in criminal proceedings has equal rights. No restrictions on rights or privileges based on race, nationality, ethnicity, gender, origin,religion, education, beliefs, political affiliation, personal and social status, or property status are permitted. (2) The court, the prosecutor and the investigating bodies shall apply the laws accurately and equally to all citizens. Other principles set up by the criminal laws are: right to defense, presumption of innocence, disclosure of objective truth, adversarial proceedings, equal rights of the parties, Independence of the bodies of criminal proceedings	art. 6-22 of the Criminal Procedure Code CONSTITUTION OF THE REPUBLIC OF BULGARIA
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	By Judge or prosecutor	
What ongoing supervision is required for the use of this tool?	The control over the implementation of the special protection is exercised by the Council for Protection of the Endangered Persons	art. 13, para 4 of the LAW ON THE PROTECTION OF PERSONS THREATENED IN CONNECTION WITH CRIMINAL PROCEEDINGS
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	N/A
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	N/A
Surveillance		
Relevant documents (legal and non-legal) that define the functioning of the tool	Law on Special Intelligence means Criminal Procedure code	
Specific range of application of the tool	The tools applies to all aspects covered in the guidance, including: Audio surveillance (Phone tapping; VOIP; Listening devices) Visual surveillance (Hidden video-surveillance devices ; body-worn video devices ; CCTV)	- Law on Special Intelligence means - Criminal procedure code

Relevant items	Provisions	Sources used
	Tracking surveillance (GPS/transponders ; mobile phones; radio-frequency identification devices (RFID)); biometric info technology) Data surveillance (computer/internet (spyware) ; mobile phones ; keystroke monitoring)	Instruction No.1 of 22/2004 on the Work and Interaction of the Preliminary Investigation Authority
How is the tool defined?	Surveillance is legally regulated in the Criminal Procedure Code (Art. 172, 1). It is defined as a one of the specific operational techniques for collecting evidence in pre-trial procedure, for prevention and detection of serious offences which according to the Law on the Special Investigation Means (Art. 5) means "visually and through technical means to detect and record various aspects of the activity and behavior of individuals and objects in their movement, residing in different locations or changes in the specific situation".	• Law on Special Intelligence means • Criminal procedure code
For what types of crime can the tool be used?	*According to art. 3 of the LSIM the Special intelligence tools (surveillance and all others) shall be used when necessary to prevent and detect serious intentional crimes under Chapter One, Chapter Two, Sections I, II, IV, V, VIII and IX, Chapter Three, Section III, Chapter Five, Sections I, VII, Chapter Six, Sections II-IV, Chapter Eight, Chapter Eight "a", Chapter Nine "a", Chapter Eleven, Sections I - IV, Chapter Twelve, Chapter Thirteen, and Chapter Fourteen, as well as for crimes under Art. 219, para. 4, proposal two, art. 220, para. 2, Art. 253, Art. 308, para. 2, 3, and 5, sentence two, art. 320, para. 2, Art. 321, Art. 321a, art. 356k and Art. 393 of the special part of the Criminal Code, when the necessary data cannot be collected in any other way or their collection is associated with exceptional difficulties. * According to art 3, some of these SOC are as follows: CRIMES AGAINST THE REPUBLIC, Murder, Injury, Kidnapping and unlawful deprivation of liberty, Coercion, Debauchery, Human Trafficking, Crimes against the political rights of citizens, Theft, Drugs, etc.	
Does national law allow this tool to be used in cross-border cases?	YES, the tool can be used both for national criminal investigation and for cross border criminal investigations	
What thresholds must be passed for the use of this tool?	* According to the Penal Code the punishments depend on the crime and could be from a financial fine to a life sentence (with parole and without parole). *For the most serious crimes, which threaten the foundations of the republic, as well as for other especially dangerous crimes (including those the controlled delivery tool applied for), the sanction is life imprisonment without parole. * The penalties are stricter when the monetary equivalent of the subject of the crime is "large amounts" or "especially large amounts". * When determining the qualifiers "large amounts" and "especially large amounts" for different types of crimes, unless otherwise specified in the law, the criteria is the monetary equivalent of the subject of the crime, which exceeds 70, respectively 140 times the minimum working salary. * However when the crime is related to taxes (tax evasion), there are other definitions for large and especially large amounts. Taxes in large amounts "are those that exceed three thousand levs (BGN 3000), and" taxes in especially large amounts "are those that exceed twelve thousand levs (BGN 12 000).	• Law on Special Intelligence means Penal Code
What types of stakeholder are involved in the implementation of this tool?	LEAs and Judicial Authorities	• Law on Special Intelligence means Criminal procedure code
Which LEAs can use this tool?	1. National Police: General Directorate "National Police", General Directorate "Fight against Organized Crime", General Directorate "Border Police", Directorate "Internal Security", regional directorates of the Ministry of Interior 2. Financial Security Unit (State Agency National Security): specialized directorates (except for "Technical Operations"), the territorial directorates and the independent territorial departments of the State Agency for National Security; 3. The Prosecutor's Office 4. The National Investigative Service 5. The Military Intelligence and Military Police services part of the Minister of Defense	Law on Special Intelligence means
What are the rules to be followed for the implementation of this tool?	A common and detailed framework of use, arrangements and application is provided in the Law on the Special Investigation Means, and at the level of secondary legislation, in Instruction No.1 of 22/2004 on the Work and Interaction of the Preliminary Investigation Authority. These legal acts define the scope of application of the wire-tapping and all other special investigation means, limited to investigation of expressly specified serious intentional offences, among which offences related to an organised criminal group, when requisite data cannot be collected in another manner or its collection involves considerable difficulties. Un application beyond pre-trial proceedings is allowed for the prevention and detection of serious intentional offences and in respect of activities related to the protection of national security. The scope of application is specified both in terms of persons and sites. These are: • persons about whom data have been received and in respect of whom a reasonable presumption can be made that they are preparing to commit, are committing, or have committed serious offences;	• Law on Special Intelligence means Criminal procedure code

Relevant items	Provisions	Sources used
	• persons about whose actions data have been received and in respect of whom a reasonable presumption can be made that they are used by the persons of the above group without being aware of the criminal nature of the activity carried out; • sites for establishment of the identity of the persons belonging to the groups referred to above; • persons and sites related to national security; • persons who have consented in writing to the use of special intelligence means for the protection of their life or property. For use of special intelligence means in pre-trial proceedings, the supervising prosecutor must submit a reasoned request in writing to the court [Criminal Procedure Code, Article 173 (1)]. Other persons who, acting within their authority, may request the use of special intelligence means and use the data and physical evidence collected by such means, are: • National Police Directorate General, Border Police Directorate General, Internal Security Directorate, regional directorates of the Ministry of Interior, and specialised directorates (with the exception of the Technical Operations Directorate), territorial directorates and stand-alone territorial departments of the State Agency for National Security; • Defence Information Service and Military Police Service under the Minister of Defence; • National Intelligence Service; • District prosecution offices for offences against political rights - buying votes (Art.167, p.3 and 4, Criminal Code) and violation of secrecy of voting(Art 169, Criminal Code). The request of the respective administrative head of the authorised institutions or the supervising prosecutor for use of special intelligence means should include following mandatory information: • complete and exhaustive indication of the facts and circumstances warranting a presumption that a serious offence is being prepared, is being committed or has been committed which necessitate the use of special intelligence means; • full description of the actions taken so far and of the results of the preliminary check or the investigation; • data identifying the persons or sites in respect of whom or which the special intelligence means are to be used; • period of use; • operational techniques, which are to be deployed; • authorised official who is to be informed of the results of the use of special intelligence means. The authorisation to use wire-tapping is granted in advance and the court is the only authority authorised to grant it. The court, which has been approached with the request, must decide immediately after receipt of the request, and the court's act together with the request are handed back to the requesting authority (Article 174 (1) to (5) of the Criminal Procedure Code and Article 15 of the Law on the Special Intelligence Means). The Criminal Procedure Code provides for the keeping of a register of the requests submitted and the authorisations granted. The legislator specifies the judicial authority to which the request must be addressed depending on the jurisdiction in terms of the investigated offence and, in certain cases, depending on the profession of the accused. The general rule is that the request should be addressed to the president of the respective district court or to a vice president expressly authorised by that president (in the case of Sofia City this would be the Sofia City Court). The special rules are as follow: - In cases to be heard by the specialised criminal court, the authorisation is granted in advance by the president of that court or by a vice president authorised by that president [Article 174 (3) of the Criminal Procedure Code]. - Authorisation to use special intelligence means in respect of members of the armed forces is granted by the president of the respective district military court or a vice president authorised by that president. - Where deployment of special intelligence means is requested in respect of a judge or the administrative head or the deputy administrative heads of a district court, the authorisation is granted by the president of the competent appellate court or a vice president expressly authorised by that president. The use of special intelligence means itself is arranged and implemented only by the respective entities: State Agency "Technical operations" and " the Specialised Directorate "Technical operations", of the State Agency for National Security Article 20 (1) of the Law on the Special Intelligence Means, as amended in 2013]. After receiving the written court permission the Chairman of the State Agency " Technical operations " or a deputy chairman designated in writing by that Chairperson gives written instruction for application of special investigative techniques. Where special investigative techniques are applied by the Specialised Directorate "Technical operations" of the State Agency for National Security, after receiving the written court permission, the Chairman of the State Agency "National Security" or a deputy chairman	

Relevant items	Provisions	Sources used
	designated in writing by that Chairperson makes a written order for the application of special investigative means.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	According to art. 57 of the Constitution of the Republic of Bulgaria (1) The fundamental civil rights are inalienable.and (2) Abuse of rights shall not be allowed. The main principle for equality is set up in the Constitution of the Republic of Bulgaria and the Criminal Procedure Code. According to art. 11 of the Criminal Procedure Code, all citizens involved in criminal proceedings has equal rights. No restrictions on rights or privileges based on race, nationality, ethnicity, gender, origin, religion, education, beliefs, political affiliation, personal and social status, or property status are permitted. (2) The court, the prosecutor and the investigating bodies shall apply the laws accurately and equally to all citizens. Other principles set up by the criminal laws are: right to defense, presumption of innocence, disclosure of objective truth, adversarial proceedings, equal rights of the parties, Independence of the bodies of criminal proceedings	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Access to the specified data is provided after authorisation by the president or by a judge authorised by the president of the regional court, which exercise jurisdiction over the head office of the requesting authority, whereupon an order to provide access to the data is issued. A special register, which is not open to public inspection, is kept at the respective regional courts for the authorisations granted or refused [Article 250c (3) of the Law on the Electronic Communications]. Depending on the crime and the subject an authorisation request for the use of this tool must be submitted to: 1. the chairmen of the Sofia City Court, 2. the respective district or military courts, 3. the specialized criminal court or to a deputy chairman authorized by them, who within 48 hours give written permission for the use of special intelligence means or refuse their use. In the cases of imminent danger of committing a serious intentional crime or in case of threat to the national security the special intelligence means may be used without permission of the body of art. 15 on the basis of an order of the Chairman of the State Agency "Technical Operations", the Chairman of the State Agency "National Security" or the Secretary General of the Ministry of Interior.	
What ongoing supervision is required for the use of this tool?	Yes it is supervised by a prosecutor. A special register, which is not open to public inspection, is kept at the Sofia City Court for the authorisations granted or refused. The respective authority of the other State is informed of the collected information according to the procedure provided for in the international treaty. Control over the application and use of special intelligence means is exercised by: 1.the Chairman of the State Agency "Technical Operations", when the special intelligence means are applied and used by the agency; 2. the Chairman of the State Agency "National Security", when the special intelligence means are applied and used by the structures of the State Agency "National Security"; 3. the Minister of Interior, when special intelligence means are used under Art. 10c ZMVR. The National Bureau for the Control of Special Intelligence Measures is an independent state body that monitors the procedures for authorization, implementation and use of special intelligence means, storage and destruction of information obtained through special intelligence means, as well as for the protection of the rights and freedoms of citizens against the illegal use of special intelligence means.	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	N/A
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	Based on the last available Report of The National Bureau for the Control of Special Intelligence Measures (page 18), surveillance tool was requested and approved as follows: * in 2019 - 4585 times *in 2018 - 4622 times *in 2017 - 3985 times	Annual Report of The National Bureau for the Control of Special Intelligence Measures Source: https://www.nbkrsr.bg/%D0%BF%D1%80%D0%BE%D0%B7%D1%80%D0%B0%D1%87%D0%BD%D0%BE%D1%81%D1%82/%D0%B4%D0%BE%D0%BA%D0%BB%D0%B0%D0%B4%D0%B8/
Undercover / covert operations		
Relevant documents (legal and non-legal) that define the functioning of the tool	Law on Special Intelligence means and the Criminal Procedure code	
How is the tool defined?	The Law on the Special Intelligence Means (Article 10c, as amended in 2013) defines an undercover officer as "an officer of the respective services under this Act, Law on the State Agency "National security", Law on the Defence and Armed Forces, or an officer of the National	• Law on Special Intelligence means Criminal procedure code

Relevant items	Provisions	Sources used
	Intelligence Service, who has been empowered to establish or to maintain contacts with a person under surveillance in order to obtain or to discover information about the commission of a serious intentional offence and about the manner in which the criminal activity is organised".	
For what types of crime can the tool be used?	"According to art. 3 of the LSIM the Special intelligence tools (covert operation and all others) shall be used when necessary to prevent and detect serious intentional crimes under Chapter One, Chapter Two, Sections I, II, IV, V, VIII and IX, Chapter Three, Section III, Chapter Five, Sections I, VII, Chapter Six, Sections II-IV, Chapter Eight, Chapter Eight ""a"", Chapter Nine ""a"", Chapter Eleven, Sections I - IV, Chapter Twelve, Chapter Thirteen, and Chapter Fourteen, as well as for crimes under Art. 219, para. 4, proposal two, art. 220, para. 2, Art. 253, Art. 308, para. 2, 3, and 5, sentence two, art. 320, para. 2, Art. 321, Art. 321a, art. 356k and Art. 393 of the special part of the Criminal Code, when the necessary data cannot be collected in any other way or their collection is associated with exceptional difficulties. * According to art 3, some of these SOC are as follows: CRIMES AGAINST THE REPUBLIC, Murder, Injury, Kidnapping and unlawful deprivation of liberty, Coercion, Debauchery, Human Trafficking, Crimes against the political rights of citizens, Theft, Drugs, etc."	
Does national law allow this tool to be used in cross-border cases?	Yes	
What thresholds must be passed for the use of this tool?	* According to the Penal Code the punishments depend on the crime and could be from a financial fine to a life sentence (with parole and without parole). *For the most serious crimes, which threaten the foundations of the republic, as well as for other especially dangerous crimes (including those the controlled delivery tool applied for), the sanction is life imprisonment without parole. * The penalties are stricter when the monetary equivalent of the subject of the crime is "large amounts" or "especially large amounts". * When determining the qualifiers "large amounts" and "especially large amounts" for different types of crimes, unless otherwise specified in the law, the criteria is the monetary equivalent of the subject of the crime, which exceeds 70, respectively 140 times the minimum working salary. * However, when the crime is related to taxes (tax evasion), there are other definitions for large and especially large amounts. Taxes in large amounts "are those that exceed three thousand leva (BGN 3000), and" taxes in especially large amounts "are those that exceed twelve thousand leva (BGN 12 000).	Law on Special Intelligence means Penal Code
What types of stakeholder are involved in the implementation of this tool?	LEAs and Judicial Authorities	
Which LEAs can use this tool?	1. National Police: General Directorate "National Police", General Directorate "Fight against Organized Crime", General Directorate "Border Police", Directorate "Internal Security", regional directorates of the Ministry of Interior 2. Financial Security Unit (State Agency National Security): specialized directorates (except for "Technical Operations"), the territorial directorates and the independent territorial departments of the State Agency for National Security; 3. The Prosecutor's Office 4. The National Investigative Service 5. The Military Intelligence and Military Police services part of the Minister of Defense	
What are the rules to be followed for the implementation of this tool?	No specific rules apply.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	According to art. 57 of the Constitution of the Republic of Bulgaria (1) The fundamental civil rights are inalienable.and (2) Abuse of rights shall not be allowed. The main principle for equality is set up in the Constitution of the Republic of Bulgaria and the Criminal Procedure Code. According to art. 11 of the Criminal Procedure Code, all citizens involved in criminal proceedings has equal rights. No restrictions on rights or privileges based on race, nationality, ethnicity, gender, origin, religion, education, beliefs, political affiliation, personal and social status, or property status are permitted. (2) The court, the prosecutor and the investigating bodies shall apply the laws accurately and equally to all citizens. Other principles set up by the criminal laws are: right to defense, presumption of innocence, disclosure of objective truth, adversarial proceedings, equal rights of the parties, Independence of the bodies of criminal proceedings	Criminal Procedure Code CONSTITUTION OF THE REPUBLIC OF BULGARIA
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	The Criminal Procedure Code requires additional mandatory information to be included in the request where an investigation through an undercover officer is requested. The head of the entity which arranges and implements this investigation, or a person authorised by this head must present to the authorising authority a declaration in writing by the officer that he or she is familiar with his or her duties and tasks under the specific investigation. The declaration is kept by the authorising authority and, instead of personal data of the officer, it states his or her personal	Law on Special Intelligence means Criminal procedure code

Relevant items	Provisions	Sources used
	identification number assigned by the entity which arranges and implements the investigation through an undercover officer (Article 173 (3)].	
What ongoing supervision is required for the use of this tool?	Leading officer or/and prosecutor	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	N/A
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	Attached is the last available Report of The National Bureau for the Control of Special Intelligence Measures (page 18). It gives some statistics regarding the different investigative tools used during the year, the number of requests and approvals for the use of the tools. According to the report, this tool was requested and approved as follows: * in 2019 - 38 times *in 2018 - 27 times *in 2017 - 28 times	Annual Report of The National Bureau for the Control of Special Intelligence Measures link.
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	The Law on the Ministry of Interior (Art. 13) Law on the State Agency for National Security (Art. 23)	
Specific range of application of the tool	No restrictions apply.	
How is the tool defined?	No legal definition of informant. The involvement of informants shall be carried out in compliance with the following principles: 1.voluntary during the attraction, work and release; 2. protection when cooperating; 3. keeping secret the identity and other data, as well as theirs activity.	• Law on the Ministry of Interior • Law on the State Agency for National Security
For what types of crime can the tool be used?	No restrictions apply.	
Does national law allow this tool to be used in cross-border cases?	Yes.	
What thresholds must be passed for the use of this tool?	No restrictions apply.	
What types of stakeholder are involved in the implementation of this tool?	LEAs and Judicial Authorities	
Which LEAs can use this tool?	Police, Customs, Financial Security Unit (State Agency National Security), The Prosecutor's Office and the National Investigative Service.	
What are the rules to be followed for the implementation of this tool?	The involvement of informants shall be carried out in compliance with the following principles: 1.voluntary during the attraction, work and release; 2. protection when cooperating; 3. keeping secret the identity and other data, as well as theirs activity.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	According to art. 57 of the Constitution of the Republic of Bulgaria (1) The fundamental civil rights are inalienable.and (2) Abuse of rights shall not be allowed. The main principle for equality is set up in the Constitution of the Republic of Bulgaria and the Criminal Procedure Code. According to art. 11 of the Criminal Procedure Code, all citizens involved in criminal proceedings has equal rights. No restrictions on rights or privileges based on race, nationality, ethnicity, gender, origin, religion, education, beliefs, political affiliation, personal and social status, or property status are permitted. (2) The court, the prosecutor and the investigating bodies shall apply the laws accurately and equally to all citizens. Other principles set up by the criminal laws are: right to defense, presumption of innocence, disclosure of objective truth, adversarial proceedings, equal rights of the parties, Independence of the bodies of criminal proceedings	• Criminal Procedure Code • CONSTITUTION OF THE REPUBLIC OF BULGARIA
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	No publicly available data on this subject.	N/A
What ongoing supervision is required for the use of this tool?	No publicly available data on this subject.	N/A
Is there any national case law relating to the use of this tool in cross-border crime cases?	No publicly available data on this subject.	N/A
Is there any data available in your country on the number of times this tool has been used for organised crime	No publicly available data on this subject.	N/A

Relevant items	Provisions	Sources used
cases? If yes can you please indicate the relevant statistics?		

Source: Author's own elaboration

Croatia

Table 21 – Overview of national rules on investigative tools - Croatia

Relevant items	Provisions	Sources used
Controlled Delivery		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Procedure Law.	https://www.legislationline.org/download/id/7895/file/Croatia_Criminal_proc_code_am2009_en.pdf
How is the tool defined?	The national law does not clearly define this tool but it says - If the investigation cannot be carried out in any other way or would be accompanied by great difficulties, the investigating judge may, upon the written request with a statement of reasons of the State attorney, order against the person against whom there are grounds for suspicion the s/he committed or has taken part in committing an offence.	Art. 332 (1) of Criminal Procedure Law. As per the Official Gazette 152/08 talks about the creating Criminal Procedure Law and also its amendments published in the Official Gazette no. 76/09. and 80/11. Class: 021-17 / 08-02 / 137, Zagreb, 11 October 2011. Edition: NN 121/2011. Document number in issue: 2386. Bearer: Committee on Legislation of the Croatian Parliament. Date of printed edition: 10/28/2011.ELI: / eli / official / 2011/121/2386. Link - https://narodne-novine.nn.hr/clanci/sluzbeni/2011_10_121_2386.html
For what types of crime can the tool be used?	This tool refer to the crimes reported in penal code- 1) offences against the Republic of Croatia (Chapter Twelve), offences against values protected by international law (Chapter Thirteen), against sexual freedom and sexual morality (Chapter Fourteen) and against the Armed Forces of the Republic of Croatia (Chapter Twenty-Six) punishable by imprisonment for a term of five years or more; 2) murder (Article 90), kidnapping (Article 125), pandering (Article 195), child pornography on a computer system or network (Article 197a), robbery (Article 218 paragraph 2), breach of confidentiality, integrity and availability of electronic data, programs and systems (Article 223), computer forgery (Article 223a), computer fraud (Article 224a), fraud to the detriment of the European Communities (Article 224b) extortion (Article 234), blackmail (Article 235), serious criminal offences against public safety (Article 271), counterfeiting of money (Article 274), money laundering (Article 279), receiving a bribe in economic transactions (Article 294a), offering a bribe in economic transactions (Article 294b), avoiding customs control (Article 298), obstruction of evidence (Article 304), duress against an official engaged in the administration of justice (Article 309), association for the purpose of committing a criminal offence (Article 333), as well as for criminal offences committed by that group or criminal organisation in concurrence, illicit possession of weapons and explosive substances (Article 335), abuse of office and official authority (Article 337), abuse in performing governmental duties (Article 338), illegal intercession (Article 343), bribe-taking (Article 347) and bribe-giving (Article 348);	Art. 334 (1), (2)
Does national law allow this tool to be used in cross-border cases?	N/A	The previous study echoes this findings
What thresholds must be passed for the use of this tool?	N/A	The previous study echoes this findings
What types of stakeholder are involved in the implementation of this tool?	LEAs	Art 332 (2)
Which LEAs can use this tool?	LEAs	Art 332 (2)
What are the rules to be followed for the implementation of this tool?	The State Attorney must give the order with a note on the time of issue and a statement of reasons to the investigating judge within eight hours from the issue. The investigating judge shall decide immediately on the legality of the order. If the investigating judge accepts the order of the State attorney, he shall proceed with executive orders to police. If the investigating judge denies the order, the State Attorney may file an appeal within eight hours.	Art 332 (2), (3), (4), (5), (6), (7)
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	No information found in the national law.	The previous study echoes this findings
What authorisation is needed for the use of this tool?	The State Attorney.	Art 332 (2)
What ongoing supervision is required for the use of this tool?	N/A	The previous study echoes this findings

Relevant items	Provisions	Sources used
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Data available on the number of times this tool has been used for SOC cases	N/A	
Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	This tool is not used	
How is the tool defined?		
For what types of crime can the tool be used?		
Does national law allow this tool to be used in cross-border cases?		
What thresholds must be passed for the use of this tool?		
What types of stakeholder are involved in the implementation of this tool?		
Which LEAs can use this tool?		
What are the rules to be followed for the implementation of this tool?		
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)		
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?		
What ongoing supervision is required for the use of this tool?		
Is there any national case law relating to the use of this tool in cross-border crime cases?		
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?		
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	Witness Protection Act.	https://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=65242&p_country=HRV&p_count=631
How is the tool defined?	No definition of this tool exists in the act. But it says - witness protection Act regulates the terms and procedures for providing protection and assistance to witness, exposed to severe danger for life, health, corporal inviolability, freedom or property of large scale arising from witnessing in criminal proceedings for criminal offences anticipated.	Art 1 (1)
For what types of crime can the tool be used?	It did not mentioned the specific crimes, but simply stated - execution of this Act is possible when there exists a possibility that a witness, due to a possible threat, would not freely testify in a criminal proceeding for grievous crimes; against the Republic of Croatia; against values protected by international law; crimes with elements of violence; organised crime and other grievous criminal offences when there were information about large scale dangers for life, health, corporal inviolability or property of the witness, while the witnessing is connected with disproportional difficulties without witnessing of endangered witness.	Art 3
Does national law allow this tool to be used in cross-border cases?	International cooperation is realised on basis of assumed rights and obligations from international treaties signed by the Republic of Croatia. International treaties may provide for relocation of endangered person outside the territory of the Republic of Croatia or reception to the territory of the Republic of Croatia.	Art 42
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	LEAs.	Art 11
Which LEAs can use this tool?	LEAs.	Art 4 (1)

Relevant items	Provisions	Sources used
What are the rules to be followed for the implementation of this tool?	Upon proposal of the competent state attorney or witness him/herselves, State Attorney General may submit request to the Board (representatives of supreme court judges) (art. 4) to include the endangered person into the Protection scheme. The following information must be included: 1) Data about the person proposed for inclusion into the protection scheme. 2) Description of criminal offence and evaluation of existing evidences. 3) Contents of possible testimony with evaluation of its importance for the proceeding. 4) Description and evaluation of danger threatening the witness.	Art 11
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	The Board (representative of supreme court judges) will provide necessary psychical, social and legal assistance to the included person. In order to assist the inclusion of included person into the new environment, the Unit will assist such a person providing economic and social support until the moment of his independence. There are no specific restrictions mentioned.	Art 34 (1), (2)
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Authorisation of board (representative of supreme court judges) is a must.	Art 4
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Surveillance		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Procedure Law.	https://narodne-novine.nn.hr/clanci/sluzbeni/2011_10_121_2386.html
Specific range of application of the tool	Audio and video.	Art 87 (1)
How is the tool defined?	Not properly defined in national law. But it says - (1) When prescribed by this Act, a trial, an evidence collecting action or any other action may be recorded by audio-video or audio recording devices.	Art 87 (1)
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross-border cases?	No.	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	State Attorney.	Chapter 13, Art 191 (1)
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	Further investigation is ongoing.	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	Audio and video.	Art 87 (1)
Undercover / covert operations		

Relevant items	Provisions	Sources used
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Procedure Law.	https://narodne-novine.nn.hr/clanci/sluzbeni/2011_10_121_2386.html
How is the tool defined?	An undercover investigator is a police officer who conducts special evidentiary actions on the order of an investigating judge.	Art 20 (1)
For what types of crime can the tool be used?	This tool refer to the crimes reported in penal code- 1) offences against the Republic of Croatia (Chapter Twelve), offences against values protected by international law (Chapter Thirteen), against sexual freedom and sexual morality (Chapter Fourteen) and against the Armed Forces of the Republic of Croatia (Chapter Twenty-Six) punishable by imprisonment for a term of five years or more; 2) murder (Article 90), kidnapping (Article 125), pandering (Article 195), child pornography on a computer system or network (Article 197a), robbery (Article 218 paragraph 2), breach of confidentiality, integrity and availability of electronic data, programs and systems (Article 223), computer forgery (Article 223a), computer fraud (Article 224a), fraud to the detriment of the European Communities (Article 224b) extortion (Article 234), blackmail (Article 235), serious criminal offences against public safety (Article 271), counterfeiting of money (Article 274), money laundering (Article 279), receiving a bribe in economic transactions (Article 294a), offering a bribe in economic transactions (Article 294b), avoiding customs control (Article 298), obstruction of evidence (Article 304), duress against an official engaged in the administration of justice (Article 309), association for the purpose of committing a criminal offence (Article 333), as well as for criminal offences committed by that group or criminal organisation in concurrence, illicit possession of weapons and explosive substances (Article 335), abuse of office and official authority (Article 337), abuse in performing governmental duties (Article 338), illegal intercession (Article 343), bribe-taking (Article 347) and bribe-giving (Article 348).	Art. 334 (1), (2)
Does national law allow this tool to be used in cross-border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	LEAs.	Art 20 (1)
What are the rules to be followed for the implementation of this tool?	Judicial Police upon requested by the state attorney.	Chapter 13, Art 191 (1)
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	No specific information about procedure is found in the law. But law stipulates that - 1) When conducting special evidentiary actions, an undercover investigator may use covert measures for the purpose of concealing the status of a police officer. 2) During the conduct of special evidence, undercover investigators and confidants may use covert audio and video devices and other technical devices to create a technical record of the conduct of special evidence.3) An undercover investigator or confidant shall give his testimony before the competent court.	- Art 21 (1) - Art 22 - Art. 23
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	The State Attorney or the investigating judge shall authorise the investigation.	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Procedure Law.	https://narodne-novine.nn.hr/clanci/sluzbeni/2011_10_121_2386.html
Specific range of application of the tool	Member of the public.	Art 202
How is the tool defined?	A trustee is a citizen who voluntarily, on the order of an investigating judge and on the instructions of the public prosecutor or the police, conducts special evidentiary actions.	Art 20 (1)
For what types of crime can the tool be used?	This tool refer to the crimes reported in penal code- 1) offences against the Republic of Croatia (Chapter Twelve), offences against values protected by international law (Chapter Thirteen), against sexual freedom and sexual morality (Chapter Fourteen) and against the Armed Forces of the Republic of Croatia (Chapter Twenty-Six) punishable by imprisonment for a term of five years	Art. 334 (1), (2)

Relevant items	Provisions	Sources used
	or more; 2) murder (Article 90), kidnapping (Article 125), pandering (Article 195), child pornography on a computer system or network (Article 197a), robbery (Article 218 paragraph 2), breach of confidentiality, integrity and availability of electronic data, programs and systems (Article 223), computer forgery (Article 223a), computer fraud (Article 224a), fraud to the detriment of the European Communities (Article 224b) extortion (Article 234), blackmail (Article 235), serious criminal offences against public safety (Article 271), counterfeiting of money (Article 274), money laundering (Article 279), receiving a bribe in economic transactions (Article 294a), offering a bribe in economic transactions (Article 294b), avoiding customs control (Article 298), obstruction of evidence (Article 304), duress against an official engaged in the administration of justice (Article 309), association for the purpose of committing a criminal offence (Article 333), as well as for criminal offences committed by that group or criminal organisation in concurrence, illicit possession of weapons and explosive substances (Article 335), abuse of office and official authority (Article 337), abuse in performing governmental duties (Article 338), illegal intercession (Article 343), bribe-taking (Article 347) and bribe-giving (Article 348).	
Does national law allow this tool to be used in cross-border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	LEAs.	Art 20 (1)
Which LEAs can use this tool?	Judicial Police upon requested by the state attorney.	Chapter 13, Art 191 (1)
What are the rules to be followed for the implementation of this tool?	1)The report shall be filed with the competent State Attorney in writing, orally or by other means.2) Undercover investigators and confidants shall compile reports on special evidentiary actions certified by the head of the police organisational unit in charge of conducting special evidentiary actions or the competent state attorney, and shall prepare documentation of the technical record of recordings made using audio and video devices.	- Art 205 (1) - Art 22 para 2
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	The State Attorney or the investigating judge shall authorise the investigation.	Art 228 (1)
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	

Source: Author's own elaboration

Cyprus

Table 22 – Overview of national rules on investigative tools - Cyprus

Relevant items	Provisions	Sources used
Controlled Delivery		
Relevant documents (legal and non-legal) that define the functioning of the tool	- The Crime Suppression (Controlled Delivery and Other Specific Provisions) Law 3(I)/1995. - RAA 17/1996. - RAA 18/1996 (Mutual Agreement signed with Russian Federation and Syrian Arab Republic). - RAA 19/1996 (Legislation entry into force on 01 February 1996).	- Greek: http://www.cylaw.org/nomoi/enop/non-ind/1995_1_3/full.html - English: https://www.imolin.org/doc/amlid/Cyprus_Law%203(I)%201995_Crime_Suppressi%20on_Act.pdf http://www.cylaw.org/KDP/data/1996_1_17.pdf http://www.cylaw.org/KDP/data/1996_1_18.pdf http://www.cylaw.org/KDP/data/1996_1_19.pdf
How is the tool defined?	"Controlled delivery" means the technique of allowing prohibited substances or prohibited articles to pass from, towards, or through the territory of one or more countries with the knowledge and under the supervision of the competent authorities with a view to identify persons involved in the commission of prescribed offences.	Art. 2 of Law 3(I)/1995

Relevant items	Provisions	Sources used
For what types of crime can the tool be used?	- Drugs, Trafficking of firearms, Financial crimes, Organised property crimes, Terrorism. - Other Offences: Explosive substances, nuclear substances.	Art. 3(2) of Law 3(I)/1995
Does national law allow this tool to be used in cross border cases?	Both national and cross-border criminal investigation.	Art 4(2), art 5 of Law 3(I)/1995
What thresholds must be passed for the use of this tool?	The tool can only be used for offences in relation prohibited substances and objects, and specifically to: - Trafficking of firearms (max. imprisonment 5 years). - Explosive substances (max. imprisonment 5 years). - Stolen articles. - Nuclear substances (max. imprisonment 10 years). - Offences outlined in Article 3(1) of the UN Convention against illicit traffic in narcotic drugs and psychotropic substances (1988) (up to imprisonment for life).	- Art. 3 of Law 3(I)/1995 - UN Convention against illicit traffic in narcotic drugs and psychotropic substances https://www.unodc.org/pdf/convention_1988_en.pdf - Law 113(I)/2004 articles 12B and 29 - Law 3(III)/1998 on the Convention for the Physical Protection of Nuclear Material (Ratification and Other Provisions) - The Drugs and Psychotropic Substances Law 29/1977
What types of stakeholder are involved in the implementation of this tool?	Police; Customs; Judicial authority.	Art 6 of Law 3(I)/1995
Which LEAs can use this tool?	Police; Customs. The same requirements/authorisations apply to both.	Art 6 of Law 3(I)/1995
What are the rules to be followed for the implementation of this tool?	Controlled delivery for prohibited substances or objects in cooperation with other countries can only take place between countries with which Cyprus has a mutual agreement. The Minister of Justice notifies those States in a Decision published in the Official Gazette. If no agreement or arrangement exists, controlled delivery may still be conducted on the basis of model terms of mutual cooperation issued by the Minister with a notification published in the Official Gazette or between Customs Services or recommendations of the World Customs Organisation	Art 5 of Law 3(I)/1995
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool?	Decision for controlled delivery must be taken by the Chief of Police and/or the Director of the Department of Customs (or their representatives which are specifically authorised for this purpose). If the decision is unilateral, the Chief of Police should notify the Director of Customs regarding its decision, and vice versa. The Attorney-General shall be informed of every decision for controlled delivery and he may give such directions as he may think necessary or appropriate.	Art. 6(2) and 6(3) of Law 3(I)/1995
What ongoing supervision is required for the use of this tool?	The legislation stipulates that controlled delivery must be executed "under the supervision of the competent authorities", but no further requirement are specified in Law 3(I)/1995. Depending on the type and nature of the substance, the relevant police unit will be in charge. For example, in cases pertaining drugs the competent authority is the Drug Law Enforcement Unit of the police.	Art. 2 of Law 3(I)/1995
Is there any national case law relating to the use of this tool in cross-border crime cases?	<u>Charalambos Hadjimarkou v Dimokratias (2002) [Supreme Court]</u>: Controlled delivery of 3kg of cannabis from Athens (Greece) to Larnaca (Cyprus) after coordination between the relevant authorities and the cooperation of the deliverer. The issue was whether the importation of cannabis under the controlled delivery scheme made such importation legal. It was held that the importation of drugs under the auspices of Law 3(I)/1995 remains an illegal importation. Thus, the appellant who induced the deliverer to transfer the drugs to Cyprus was found guilty and his appeal was dismissed. <u>Kleomenis Marios v Dimokratias (2013) [Supreme Court]</u>: The Drug Law Enforcement Unit of the Cyprus Police was informed that a package containing drugs would be delivered from India to Cyprus. The Unit found 2,3kg of cannabis in the package hidden within four wooden frames. It removed the illegal substance from the package, which was ultimately delivered to its recipient. The issue was whether removing the whole of the illegal substance, without substituting it with another substance (e.g. a cannabis look-alike) could amount to controlled delivery according to the provisions of article 4(3) of the Law. The court held that removal without replacement could not amount to controlled delivery, and the recipient was acquitted from the charge of possession. <u>Christos Toumazou v Dimokratias (2015) [Supreme Court]</u>: The competent authorities of Slovakia identified a package which contained 5kg of cannabis that was about to be delivered in Cyprus and informed the national authorities. The Slovakian authorities substituted the illegal substance with paper, and when the package was delivered in Cyprus, the Drug Law Enforcement Unit substituted the paper with soil of equal weight. The issue was whether the Controlled Delivery Law prohibits the substitution of the drugs to take place in the country of receipt (Cyprus). The argument was rejected, as it was held substitution can take place in the country of receipt and the appeal was dismissed. <u>Michali Michael v Dimokratias (2018) [Supreme Court]</u>: The case involved the delivery of 15,9kg of cannabis from the Netherlands to Cyprus via Germany. After communication between the German and Cypriot authorities, the former intercepted the package to remove the prohibited substance, while the latter inserted a substituted substance in the package. The appellant was found guilty for the charges of possession and possession	- Kleomenis Marios v Dimokratias (2013) [Supreme Court] http://www.cylaw.org/cgi-bin/open.pl?file=apofaseis/aad/meros_2/2013/rep/2013_2_0350.htm&qstring=%F0%E5%F1%E9%20and%20%EA%E1%F4%E1%F3%F4%EF%EB%2A%20and%20%F4%EF%F5%20and%20%E5%E3%EA%EB%E7%EC%E1%2A%20and%20%22%E5%EB%E5%E3%F7%EF%EC%E5%ED%2A%20and%20%F0%E1%F1%E1%E4%EF%F3%2A%22%20and%20%2295%22 - Charalambos Hadjimarkou v Dimokratias (2002) [Supreme Court] http://www.cylaw.org/cgi-bin/open.pl?file=apofaseis/aad/meros_2/2002/rep/2002_2_0482.htm&qstring=%F0%E5%F1%E9%20and%20%EA%E1%F4%E1%F3%F4%EF%EB%2A%20and%20%F4%EF%F5%20and%20%E5%E3%EA%EB%E7%EC%E1%2A%20and%20%22%E5%EB%E5%E3%F7%EF%EC%E5%ED%2A%20and%20%F0%E1%F1%E1%E4%EF%F3%2A%22%20and%20%2295%22 - Christos Toumazou v Dimokratias (2015) [Supreme Court] http://www.cylaw.org/cgi-bin/open.pl?file=apofaseis/aad/meros_2/2015/2-201512-142-14.htm&qstring=%F0%E5%F1%E9%20and%20%EA%E1%F4%E1%F3%F4%EF%EB%2A%20and%20%F4%EF%F5%20and%20%E5%E3%EA%EB%E7%EC%E1%2A%20and%20%22%E5%EB%E5%E3%F7%EF%EC%E5%ED%2A%20and%20%F0%E1%F1%E1%E4%EF%F3%2A%22%20and%20%2295%22

Relevant items	Provisions	Sources used
	with the intent to distribute the drug. For possession to be committed upon receipt, the provisions of article 4(3) of the Law must apply (receiving the substituted substance is considered to be receipt of the prohibited substance). It was argued that this provision was inapplicable because according to article 4(2) such the substitution has to be made for "prohibited substances... imported or trafficked in Cyprus". Ergo, since the package arrived in Cyprus empty of drugs, its receipt by the appellant after the insertion of a substituted substances should not be considered to be receipt of the prohibited substance. Thus, the issue was whether the prohibited substance had to be imported in Cyprus for its substitution to fall under the scope of article 4(3). The court held that both the seizure and replacement of the prohibited substance can take place either inside or outside Cyprus. The appeal was dismissed.	
Data available on the number of times this tool has been used for SOC cases	N/A	
Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	N/A	
How is the tool defined?	N/A	
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross-border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	The Witness Protection Law 95(I)/2001.	The Witness Protection Law 95(I)/2001
How is the tool defined?	It is the protection of witnesses that are in need assistance during criminal proceedings. A witness can be in need of assistance if one of the following applies: • The witness is than 18 years old. • The witness suffers mental or physical difficulties. • The Court considers that the quality of the witness' testimony susceptible of being compromised due to fear, anxiety or distress. • The Attorney General has enrolled the witness into the Witness Protection Scheme.	• Article 3 of Law 95(I)/2001
For what types of crime can the tool be used?	For any criminal proceeding.	• Article 3 of Law 95(I)/2001
Does national law allow this tool to be used in cross-border cases?	National criminal investigation.	
What thresholds must be passed for the use of this tool?	Life sentence.	

Relevant items	Provisions	Sources used
What types of stakeholder are involved in the implementation of this tool?	Courts; Attorney General.	Articles 3 and 16 of Law 95(I)/2001
Which LEAs can use this tool?	Judiciary.	Articles 3 and 16 of Law 95(I)/2001
What are the rules to be followed for the implementation of this tool?	The Court considers whether a witness is in need of assistance, it contemplates what protection measures are appropriate given the nature of the case, and issues a relevant order for their enforcement. Alternatively, the Attorney General may opine that a witness or other person should be enrolled in the Witness Protection Scheme.	Article 4 and 17 of Law 95(i)/2001
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	No witness can be enrolled to the Witness Protection Scheme without his consent as to the enrolment per se and the protected measures he will be subjected to.	Article 16(4) of Law 95(I)/2001
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	The Court considers whether a witness is in need of assistance, it contemplates what protection measures are appropriate given the nature of the case, and issues a relevant order for their enforcement. Alternatively, the Attorney General may opine that a witness or other person should be enrolled in the Witness Protection Scheme.	Article 4 and 17 of Law 95(i)/2001
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Surveillance		
Relevant documents (legal and non-legal) that define the functioning of the tool	The law prescribes that any device can be used for any type of surveillance (audio, visual, tracking or data), except for devices that are used by the person in the ordinary course of their work or devices that are used for hearing aid.	Art 2 of Law 92(I)/1996
Specific range of application of the tool	"Surveillance" means the acoustic or otherwise means of receiving the contents of any private communication using any electronic, mechanical, electromagnetic, acoustic or other device or machine and includes listening, recording or any other form of recording or recording the contents of such communication or whole or in part either in substance or in its meaning or concept or purpose	Art 2 of Law 92(I)/1996
How is the tool defined?	Surveillance of private communications can be utilised: a) When it is in the interest for the security of the State; b) To prevent, investigate or prosecute: Premeditated murder or homicide; trafficking in adults or minors and offenses related to child pornography; the marketing, supply, cultivation or production of narcotic drugs, psychotropic substances or dangerous drugs; offenses related to the currency or banknote of the Republic; and corruption offenses for which, in the event of a conviction, a prison sentence of five years or more is provided.	Art 6(2) of Law 92(I)/1996
For what types of crime can the tool be used?	Both national and cross-border criminal investigations. Another country may submit a written request for obtaining a testimony within the Republic of Cyprus. The request must be: - In relation to proceedings which have started before the national court of that particular country. - In relation to an ongoing criminal investigation of that particular country. - Must be for the surveillance of private communications.	Art 8A of Law 92(I)/1996
Does national law allow this tool to be used in cross-border cases?	Surveillance of private communications can be utilised: a) When it is in the interest for the security of the State. b) To prevent, investigate or prosecute: Premeditated murder or homicide; trafficking in adults or minors and offenses related to child pornography; the marketing, supply, cultivation or production of narcotic drugs, psychotropic substances or dangerous drugs; offenses related to the currency or banknote of the Republic; and corruption offenses for which, in the event of a conviction, a prison sentence of five years or more is provided. Maximum term of imprisonment of crimes for which the tool can be used: life sentence.	Art 6(2) of Law 92(I)/1996
What thresholds must be passed for the use of this tool?	Police and/or Cyprus Information Service; Judicial Authority.	Art 6 and 6A of Law 92(I)/1996
What types of stakeholder are involved in the implementation of this tool?	Police; Cyprus Information Service.	Art 6 and 6A of Law 92(I)/1996

Relevant items	Provisions	Sources used
Which LEAs can use this tool?	The rules to be followed by persons authorised to conduct surveillance activities are delineated in the Court Order, and may differ depending on the situation at hand. Authorised persons which act beyond their demarcated scope of competence as prescribed in the court order, are committing an offence which is punishable by imprisonment not exceeding 5 years or a fine not exceeding EUR 50.000.	- Art 8 of Law 92(I)/1996 - Art 6A(4) of Law 92(I)/1996
What are the rules to be followed for the implementation of this tool?	No specific provision.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	The Attorney General, upon the written request of the Chief of Police or the Commander of the CIS or any investigator, submits an ex ante application to the Court, requesting the issuance of a court order authorizing the surveillance of private communication by authorised persons. Such persons are members of the police/CIS or perform duties for their service, which receive written authorisation by the Chief of Police or the CIS Commander accordingly.	Art 6(1) and 6A(1) of Law 92(I)/1996
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	When issuing a court order, the judge may prescribe that the CIS Commander or the Chief of Police, as the case may be, shall inform the Attorney General about the progress of the ongoing surveillance.	Art 12 of Law 92(I)/1996
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Undercover / covert operations		
Relevant documents (legal and non-legal) that define the functioning of the tool	The law only defines: "Operation" as a secret mission of the police for the purposes of preventing or investigating serious criminal offences. "Covert officer" as a member of the police whose identity is not disclosed to third parties and who is specifically trained and acts as a source of information or conducts an investigation.	Art 2 of Law 189(I)/2017
How is the tool defined?	Cross crime areas	Art 2 of Law 189(I)/2017
For what types of crime can the tool be used?	An authorisation for a member of the police to operate as a covert officer may extend to the territory of another Member State or third country, pursuant to any international treaty ratified by a relevant ratifying Cypriot law, and with the consent and cooperation of the competent authorities of the Member State or third country. The Attorney General may authorise the operation of a covert officer from another Member State or third country, pursuant to the provisions of Law on Joint Investigation Teams (244(I)/2004) or a ratified international treaty respectively.	Art 3(7) and 3(10) of Law 189(I)/2017
Does national law allow this tool to be used in cross-border cases?	Covert operations are only conducted for the prevention or investigation of serious criminal offences, which are punishable by three years of imprisonment or more.	Art 2 of Law 189(I)/2017
What thresholds must be passed for the use of this tool?	Police.	Law 189(I)/2017
What types of stakeholder are involved in the implementation of this tool?	Police.	Law 189(I)/2017
Which LEAs can use this tool?	An Investigating Officer which holds at least the rank of Sergeant, requests from an Authorizing officer (the Police Director of a Province or Department or the Commander of a Unit or Service or the Assistant Chief of Operations or his / her Deputy), to receive authorisation to use a member of the police as a covert officer. Once such an authorisation is granted, the Investigating Officer can elect a covert officer, provided that the latter has given his/her prior consent and received the appropriate special training.	Articles 4,6 and 7 of Law 189(I)/2017
What are the rules to be followed for the implementation of this tool?	The Investigating Officer must explain in the request why he/she believes that the authorisation of a covert operation is necessary proportionate to the intended purpose of the case at hand. In order for the Authorizing Officer to grant authorization, he/she must be satisfied that the covert operation is necessary and proportionate to the intended purpose of the case. In order for the Authorizing Officer to grant authorisation, he/she must be satisfied that the covert operation is necessary and proportionate to the intended purpose of the case.	Articles 3(6) and 4(2) of Law 189(I)/2017
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	An Investigating Officer which holds at least the rank of Sergeant, requests from an Authorizing officer (the Police Director of a Province or Department or the Commander of a Unit or Service or the Assistant Chief of Operations or his / her Deputy), to receive authorisation to use a member of the police as a covert officer. Once such an authorisation is granted, the Investigating Officer	Articles 4,6 and 7 of Law 189(I)/2017

Relevant items	Provisions	Sources used
	can elect a covert officer, provided that the latter has given his/her prior consent and received the appropriate special training.	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	The Investigating officer supervises the covert operation.	Art. 5 of Law 189(I)/2017
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	N/A	
Specific range of application of the tool	N/A	
How is the tool defined?	N/A	
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross-border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	

Source: Author's own elaboration

Czechia

Table 23 – Overview of national rules on investigative tools - Czechia

Relevant items	Provisions	Sources used
Controlled Delivery		
Relevant documents (legal and non-legal) that define the functioning of the tool	Code of Criminal Procedure Act No. 141/1961 Coll. Article 86, 87, 87a, 87b, 87c.	https://www.zakonyprolidi.cz/cs/1961-141
How is the tool defined?	If it is necessary to ascertain the contents of undelivered mail consignments, other consignments or telegrams to clarify the facts important for criminal proceedings in a particular matter, the	Code of Criminal Procedure Act No. 141/1961 Coll. Article 86, 87, 87a, 87b, 87c

Relevant items	Provisions	Sources used
	presiding judge and in pre-trial proceedings the public prosecutor shall order the post office or the person performing their transport to deliver consignment to the presiding judge and in pre-trial proceedings either to the public prosecutor or police body. There are four institutes - 1) detention of consignment, 2) opening of consignment, 3) consignment substitution, 4) monitored consignment.	
For what types of crime can the tool be used?	Respective Provision of the Code of Criminal Procedure reads as follows: In the interest of ascertaining the persons participating in disposing of a consignment containing narcotics, psychotropic substances, precursors, toxins, radioactive materials, forged money and forged securities, firearms or weapons of mass destruction, ammunition and explosives or any other specific object for possession of which a special permit is required by law, specific object intended for committing a crime or specific object related to criminal activity. The presiding judge, or in pre-trial proceedings the public prosecutor with the consent of the presiding judge, may order to substitute the content of the consignment with different content and such adjusted consignment to be given for further transport. The aim of this action is to identify final recipient of such consignment. The Police Forces will arrange the consignment substitution and its delivery.	Code of Criminal Procedure Act No. 141/1961 Coll. Article 87a (paragraph 1)
Does national law allow this tool to be used in cross-border cases?	National law does not specifically point to this direction, but based on application of the national law, rule that is not negatively listed, the rule can be applicable, unless stated other ways.	Code of Criminal Procedure Act No. 141/1961 Coll. Article 86 - 87c
What thresholds must be passed for the use of this tool?	National law does not provide a specification in respect of length of the prison sentence.	Code of Criminal Procedure Act No. 141/1961 Coll. Article 86 - 87c
What types of stakeholder are involved in the implementation of this tool?	In the pre-trial proceedings, the public prosecutor may order that a consignment which is reasonably suspected of containing objects mentioned in Section 87, to be monitored if necessary for clarification of the crime or to identify all its recipients, in case other possible action may fail or might not be sufficient to obtain necessary adequate results. In case the warrant is not issued prior the monitoring, Police Forces are allowed, on their own, monitor the consignment however, the warrant must be issued as soon as possible.	Code of Criminal Procedure Act No. 141/1961 Coll. Article 87b (paragraph 1)
Which LEAs can use this tool?	Presiding judge and in pre-trial proceedings the public prosecutor shall order the post office or the person performing their transport to deliver consignment to the presiding judge and in pre-trial proceedings either to the public prosecutor or police body.	Code of Criminal Procedure Act No. 141/1961 Coll. Article 87b (paragraph 1 & 2)
What are the rules to be followed for the implementation of this tool?	Based on the approval from Public Prosecutor, Police Forces acts on their respective competencies towards "Controlled Delivery" according to the Code of the Criminal Procedure.	Code of Criminal Procedure Act No. 141/1961 Coll. Article 87b (paragraph 1)
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Detailed rules for the implementation of the tool are restricted for Personnel of the respective units and are not publicly available.	
What authorisation is needed for the use of this tool?	Particular law does not include any specific additional protection. All actions by the Police Forces can be addressed and scrutinised by the General Inspectorate of Security Forces (GIBS), or by the Court.	
What ongoing supervision is required for the use of this tool?	The public prosecutor may order in the preliminary proceedings that a consignment in respect of which there is justified suspicion that it contains items such as, (narcotics, psychotropic substances, precursors, toxins, radioactive materials, forged money and forged securities, firearms or weapons of mass destruction, ammunition and explosives or any other specific object for possession of which a special permit is required by law, specific object intended for committing a crime or specific object related to criminal activity), if it is necessary to clarify a criminal offence or discovery of all its offenders and ascertaining required circumstance in another manner would be ineffective, or substantially more difficult. The Police Forces will arrange monitoring of the consignment according to the public prosecutor's instruction; no performance aimed at surrendering or withdrawing the object are executed with regards to person who handle the monitored consignment, and a protocol or another record is required. The police Forces may initiate monitoring of a consignment without prior authorisation, (In case the warrant is not issued prior the monitoring, Police Forces is able, on their own, monitor the consignment however, the warrant must be issued as soon as possible by the Public Prosecutor or Judge) The police Forces advises the public prosecutor thereof without delay and proceeds further according to the instruction. The Police Forces may take up required measures to achieve their objective or intercept particular consignment, which is leaving the geographic area of Czechia abroad, and vice versa, or from abroad via the geographic area of Czechia to another third country.	Code of Criminal Procedure Act No. 141/1961 Coll. Article 87b (paragraph 1 & 2)
Is there any national case law relating to the use of this tool in cross-border crime cases?	The warrant for the controlled delivery shall be issued by the presiding judge; before the commencement of criminal proceedings or in the preparatory proceedings by the prosecutor.	Code of Criminal Procedure Act No. 141/1961 Coll. Article 86 (paragraph 1)
Data available on the number of times this tool has been used for SOC cases	N/A	
Hot pursuit		

Relevant items	Provisions	Sources used
Relevant documents (legal and non-legal) that define the functioning of the tool	• Schengen Agreement Article 41. • Bilateral agreements on cross-border police cooperation with SK, AT, DE and PL. • Act on Police Force of Czechia 273/2008 Coll. Article 93.	• https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A42000A0922%2802%29 • https://www.zakonyprolidi.cz/cs/2008-273
How is the tool defined?	Officers of one of the Contracting Parties who are pursuing in their country an individual caught in the act of committing or of participating in one of the offences referred to in paragraph 4 shall be authorised to continue pursuit in the territory of another Contracting Party without the latter's prior authorisation where, given the particular urgency of the situation, it is not possible to notify the competent authorities of the other Contracting Party by one of the means provided for in Article 44 prior to entry into that territory or where these authorities are unable to reach the scene in time to take over the pursuit. Article 44 1. In accordance with the relevant international agreements and account being taken of local circumstances and technical possibilities, the Contracting Parties shall install, in particular in border areas, telephone, radio, and telex lines and other direct links to facilitate police and customs cooperation, in particular for the timely transmission of information for the purposes of cross-border surveillance and hot pursuit. 2. In addition to these short-term measures, they will in particular consider the following options: a) Exchanging equipment or posting liaison officers provided with appropriate radio equipment. b) Widening the frequency bands used in border areas. c) Establishing common links for police and customs services operating in these same areas. d) Coordinating their programmes for the procurement of communications equipment, with a view to installing standardised and compatible communications systems.	• Schengen Agreement Article 41 (paragraph 1) and Article 44
For what types of crime can the tool be used?	• The following criminal offences: murder, manslaughter, rape, arson, forgery of money, aggravated burglary and robbery and receiving stolen goods, extortion, kidnapping and hostage taking, trafficking in human beings, illicit trafficking in narcotic drugs and psychotropic substances, breach of the laws on arms and explosives, wilful damage through the use of explosives, illicit transportation of toxic and hazardous waste, failure to stop and give particulars after an accident which has resulted in death or serious injury. • Extraditable offences.	• Schengen Agreement Article 41 (paragraph 4 a/b)
Does national law allow this tool to be used in cross-border cases?	National law as well as Schengen Agreement allow the tool to be used in Cross-border cases.	• Schengen Agreement Article 41 • Bilateral agreements on cross-border police cooperation with SK, AT, DE and PL. • Act on Police Force of Czechia 273/2008 Coll. Article 93
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	The pursuing Police Officers shall, not later than when they cross the border, contact the competent authorities of the Contracting Party in whose territory the hot pursuit will take place.	• Schengen Agreement Article 41 (paragraph 3)
Which LEAs can use this tool?	Police Force. There is no specific mention of this mechanism in the criminal procedure code, just a general reference in Article 93 of the Police force act , stipulating that a member of the Czech police force could carry out hot pursuit on the territory of another state on the basis of an international treaty. The same regulation is valid also for police officers from other countries to carry out their powers on the territory of Czechia.	• Act on Police Force of Czechia 273/2008 Coll. Article 93
What are the rules to be followed for the implementation of this tool?	Officers of one of the Contracting Parties who are pursuing in their country an individual caught in the act of committing or of participating in one of the offences referred to in paragraph 4 shall be authorised to continue pursuit in the territory of another Contracting Party without the latter's prior authorisation where, given the particular urgency of the situation. Detailed rules for the implementation of the tool are restricted for Personnel of the respective units and are not publicly available.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Particular law does not include any specific additional protection. All actions by the Police Forces can be addressed and scrutinised by the General Inspectorate of Security Forces (GIBS), or by the Court.	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	The pursuing officers shall, not later than when they cross the border, contact the competent authorities of the Contracting Party in whose territory the hot pursuit is to take place. The hot pursuit will cease as soon as the Contracting Party in whose territory the pursuit is taking place so requests. At the request of the pursuing officers, the competent local authorities shall challenge the pursued person in order to establish the person's identity or to make an arrest.	
What ongoing supervision is required for the use of this tool?	Tool does not require judicial supervision. Rules given by the Schengen Agreement and respective Bilateral Agreements need to be followed. Internal approval within the Police Force are subject to respective internal rules and regulation and are not publicly available.	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this	N/A	

Relevant items	Provisions	Sources used
tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?		
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	Act on special protection of witnesses and other persons in connection with criminal proceedings - 137/2001 Coll.	https://www.zakonyprolidi.cz/cs/2001-137
How is the tool defined?	Special protection and assistance is a set of measures that include: - Personal protection. - Relocation of the protected person, including members of his / her household and assistance to the protected person for the purpose of his / her social integration in the new environment. - Concealing the real identity of the protected person. - Verifying compliance with the conditions for granting special protection and assistance.	Act on special protection of witnesses and other persons in connection with criminal proceedings - 137/2001 Coll. Article 3 (paragraph 1)
For what types of crime can the tool be used?	National law explicitly do not provide information about what crime needs to be committed, for this tool to be applicable. Professional judgement is exercised case by case.	
Does national law allow this tool to be used in cross-border cases?	- Within the framework of international cooperation, classified information shall be provided abroad without the consent of the competent state authority. - Special protection and assistance may also be provided based on the request of competent authority of a foreign state, which decides on the protection of a person under the law of a foreign state (hereinafter "authority of a foreign state"), or at the request of an international criminal court, international criminal tribunal. , or a similar international judicial body, which meet at least one of the conditions specified in Article 145 (paragraph 1) of Act on International Judicial Cooperation in Criminal Matters.	- Act on special protection of witnesses and other persons in connection with criminal proceedings - 137/2001 Coll. Article 21 (paragraph 1) - Act on special protection of witnesses and other persons in connection with criminal proceedings - 137/2001 Coll. Article 1 (paragraph 3)
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	- The Minister of the Interior shall approve the proposal from the Police Forces/ judge or prosecutor makes such a proposal through the Minister of Justice - where special protection and assistance will be provided to the witness. - If the witness is in immediate threat to life, the Police Forces with the consent from Police President or the Prison Service with the consent of the Director General of the Prison Service shall exercise special protection and assistance to witness.	- Act on special protection of witnesses and other persons in connection with criminal proceedings - 137/2001 Coll. Article 4 (paragraph 1, section b) - Act on special protection of witnesses and other persons in connection with criminal proceedings - 137/2001 Coll. Article 4 (paragraph 4)
Which LEAs can use this tool?	- The Minister of the Interior shall approve the proposal from the Police Forces/ judge or prosecutor makes such a proposal through the Minister of Justice - where special protection and assistance will be provided to the witness. - If the witness is in immediate threat to life, the Police Forces with the consent from Police President or the Prison Service with the consent of the Director General of the Prison Service shall exercise special protection and assistance to witness.	- Act on special protection of witnesses and other persons in connection with criminal proceedings - 137/2001 Coll. Article 4 (paragraph 1, section b) - Act on special protection of witnesses and other persons in connection with criminal proceedings - 137/2001 Coll. Article 4 (paragraph 4)
What are the rules to be followed for the implementation of this tool?	For the purpose of Act 137/2001, is to provide special protection and assistance to witnesses who, in connection with criminal proceedings, are likely to be at risk or threat to life.	Act on special protection of witnesses and other persons in connection with criminal proceedings - 137/2001 Coll. Article 1 (paragraph 1)
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Particular law does not include any specific additional protection. All actions by the Police Forces can be addressed and scrutinised by the General Inspectorate of Security Forces (GIBS), or by the Court.	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	- The Minister of the Interior shall approve the proposal from the Police Forces/ judge or prosecutor makes such a proposal through the Minister of Justice - where special protection and assistance will be provided to the witness. - If the witness is in immediate threat to life, the Police Forces with the consent from Police President or the Prison Service with the consent of the Director General of the Prison Service shall exercise special protection and assistance to witness.	- Act on special protection of witnesses and other persons in connection with criminal proceedings - 137/2001 Coll. Article 4 (paragraph 1, section b) - Act on special protection of witnesses and other persons in connection with criminal proceedings - 137/2001 Coll. Article 4 (paragraph 4)
What ongoing supervision is required for the use of this tool?	National Legislation does not stipulate any specific ongoing supervision over this tool. Internal regulations and procedures are restricted for the personal of the respective units and are not publicly available.	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Surveillance		

Relevant items	Provisions	Sources used
Relevant documents (legal and non-legal) that define the functioning of the tool	- Code of criminal procedure 141/1961 Coll. Article 88, 88a, 158d (physical/electronic - procedural) - Act on Police Force 273/2008 Article 98 (physical/electronic - operative)	https://www.zakonyprolidi.cz/cs/1961-141 https://public.psp.cz/en/sqw/hp.sqw?k=7609 https://www.zakonyprolidi.cz/cs/2008-273
Specific range of application of the tool	Surveillance of person and/or object (hereafter "surveillance") is regulated by Section 158d of the Act No. 141/1961 Coll. (Code of Criminal Procedure) and is understood as obtaining knowledge of persons and objects in a secret manner by technical and other means. If, during surveillance, the police body finds that an accused person is communicating with his/her counsel, the Police Forces is obliged to destroy the record of the communication.	Code of criminal procedure 141/1961 Coll. Article 158d
How is the tool defined?	Tracking of a person and thing (hereinafter referred to as "tracking") means the acquisition of information on the movement and activity of a person or movement, which is carried out in a classified manner; surveillance may be carried out in criminal proceedings concerning an intentional criminal offense, if it can be reasonably assumed that it will establish facts relevant to the criminal proceedings.	Code of criminal procedure 141/1961 Coll. Article 158 (paragraph d, section 1)
For what types of crime can the tool be used?	- If criminal proceedings are conducted for a crime for which the law provides for imprisonment with a maximum penalty of at least eight years, for the crime of conspiracy in insolvency proceedings pursuant to Article 226 of the Criminal Code, violation of regulations on competition rules pursuant to Article 248 paragraph 1 section e) and paragraphs 2 to 4 of the Criminal Code, arranging an advantage when awarding a public contract, in a public tender and public auction according to Article 256 of the Criminal Code Article 258 of the Criminal Code, abuse of power by an official pursuant to Article 329 of the Criminal Code, false accusation pursuant to Article 345 paragraph 3 to 5 of the Criminal Code, false statement and false expert opinion pursuant to Article 346 paragraph 3 to 5 of the Criminal Code or for another intentional criminal offense, the prosecution of which is bound by a promulgated international treaty, an order may be issued to intercept and record telecommunications traffic if it can be reasonably assumed that it will obtain significant facts for criminal proceedings and if the observed otherwise or if it would be significantly more difficult to achieve. - If, for the purposes of criminal proceedings conducted for an intentional criminal offense for which the law provides for imprisonment with a maximum penalty of at least three years, it is necessary for the criminal offense of violating the secrecy of transported messages (Article 182 of the Criminal Code), for a criminal offense of fraud (Article 209 of the Criminal Code), for the offense of unauthorised access to a computer system and information carrier (Article 230 of the Criminal Code), for the offense of measures and storage of an access device and password to a computer system and other such data (Article 231 of the Criminal Code), for the criminal offense of dangerous threat (Article 353 of the Criminal Code), for the criminal offense of dangerous persecution (Article 354 of the Criminal Code), for the criminal offense of spreading an alarm message (Article 357 of the Criminal Code), for the criminal offense of unobjecting to a criminal offense (Article 364 of the Criminal Code), for the criminal offense of approving a criminal offense (Article 365 of the Criminal Code), or for an intentional criminal offense, the prosecution of which is bound by a promulgated international treaty, which Czechia is bound to find out data on telecommunication traffic which are the subject of telecommunication secrecy or which are covered by the protection of personal and intermediary data and if the intended purpose cannot be achieved otherwise or if its achievement would otherwise be significantly more difficult.	- Code of criminal procedure 141/1961 Coll. Article 88 (paragraph 1) - Code of criminal procedure 141/1961 Coll. Article 88a (paragraph 1)
Does national law allow this tool to be used in cross-border cases?	Office for Foreign Relations and Information (Intelligence Service), its director is authorised to use operational investigative means in proceedings on an intentional criminal offense for tracking of persons and things.	Code of criminal procedure 141/1961 Coll. Article 158b (paragraph 1)
What thresholds must be passed for the use of this tool?	- If criminal proceedings are conducted for a crime for which the law provides for imprisonment with a maximum penalty of at least eight years. - If, for the purposes of criminal proceedings conducted for an intentional criminal offense for which the law provides for imprisonment with a maximum penalty of at least three years.	- Code of criminal procedure 141/1961 Coll. Article 88 (paragraph 1) - Code of criminal procedure 141/1961 Coll. Article 88a (paragraph 1)
What types of stakeholder are involved in the implementation of this tool?	Police authorities respectively to their competencies according to the Code of the Criminal Procedure.	Code of criminal procedure 141/1961, Article 88, 88a, 158d
Which LEAs can use this tool?	The agencies that are allowed to use the tool of surveillance are divided between judicial authorities, such as president of the senate, prosecutor and executive power such as Police Forces.	Code of criminal procedure 141/1961 Coll. Article 88 (paragraph 2,3 & 4)
What are the rules to be followed for the implementation of this tool?	Permission under can be issued only on the basis of an application in writing. The application must be justified by suspicion of specific criminal activity and also, if it is known, data on the persons or objects which are to be placed under surveillance. The time for which surveillance will be carried out and which may not exceed six months must be stipulated in the permission. The person who has allowed surveillance may, on the basis of a new application in writing, extend this period always for at most six months. The police body is, however, obliged to apply without	Code of criminal procedure 141/1961 Coll. Article 158d (paragraph 4 & 5)

Relevant items	Provisions	Sources used
	delay for permission thereafter, and if this is not obtained within 48 hours, is obliged to terminate surveillance, destroy any record and in no way use the information learned in connection with it.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Particular law does not include any specific additional protection. All actions by the Police Forces can be addressed and scrutinised by the General Inspectorate of Security Forces (GIBS), or by the Court.	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	- The surveillance order is issued in writing by the President of the Senate, before the commencement of criminal prosecution or in preparatory proceedings by the public prosecutor. - Acts under § 88 and § 158d of the Criminal Procedure Code related to wiretapping and tracking are important tools for detecting, investigating and investigating the most serious forms of crime, such as abuse of power, corruption, organised crime, drug, violent or moral crime and as such are subjects to the control of The Standing Commission for the for the Control of the Use of Eavesdropping and Recording of Telecommunication Traffic, the Use of Tracking of Persons and Things and the Interruption of Electronic Communications.	- Code of criminal procedure 141/1961 Coll. Article 158d (paragraph 2,3 & 5) - The Standing Commission for the Control of the Use of Eavesdropping and Recording of Telecommunication Traffic, the Use of Tracking of Persons and Things and the Interruption of Electronic Communications is a control body of the Chamber of Deputies, established pursuant to Act No. 273/2008 Coll., On the Czech Police.
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	Some examples relating to the use of the tool can be found in the Annual Report of Czech police National Agency against Organised Crime.	https://www.policie.cz/clanek/web-informacni-servis-zpravodajstvi-vyrocní-zprava-ncoz-2019.aspx
Undercover / covert operations		
Relevant documents (legal and non-legal) that define the functioning of the tool	Code of Criminal Procedure Act No. 141/1961 Coll., Article 158b ; 158e	https://www.zakonyprolidi.cz/cs/1961-141
How is the tool defined?	An agent is an officer of the Czech Police or of General Inspection of Security Forces carrying out tasks assigned to him/her by the police authority, usually involving concealment of the actual purpose of his/her activity. If criminal proceedings are being conducted for the crime for which the law provides imprisonment for a term of at least eight years, for a crime conducted on behalf of organized criminal group, for a crime of conniving in insolvency proceedings, infringement of the competition rules, negotiate benefits for the award of public contracts, public tender or public auction, conniving at the award of a contract in a competitive tender, conniving at public auction, abuse of power of an official, acceptance of a bribe, bribery, indirect bribery or for any other intentional crime the prosecution of which is an obligation resulting from a promulgated international treaty binding on Czechia, the police authority, if it is a unit of the Police of Czechia or General Inspection of Security Forces, is entitled to use an agent. If proceedings are being conducted for the crime for which the law provides imprisonment for a term of at least eight years, for a crime conducted on behalf of organised criminal group, for a crime of conniving in insolvency proceedings, infringement of the competition rules, negotiate benefits for the award of public contracts, public tender or public auction, conniving at the award of a contract in a competitive tender, conniving at public auction, abuse of power of an official, acceptance of a bribe, bribery, indirect bribery or for any other intentional crime the prosecution of which is an obligation resulting from a promulgated international treaty binding on Czechia, the police authority, if it is a unit of the Police of Czechia or General Inspection of Security Forces, is entitled to use an agent.	Code of Criminal Procedure Act No. 141/1961 Coll. Article 158e (paragraph 1 & 2)
For what types of crime can the tool be used?	The tool is used for any of these following scenarios: Crime conducted on behalf of organised criminal group, for a crime of conniving in insolvency proceedings, infringement of the competition rules, negotiate benefits for the award of public contracts, public tender or public auction, conniving at the award of a contract in a competitive tender, conniving at public auction, abuse of power of an official, acceptance of a bribe, bribery, indirect bribery or for any other intentional crime.	Code of Criminal Procedure Act No. 141/1961 Coll. Article 158e (paragraph 1)
Does national law allow this tool to be used in cross-border cases?	Use of an agent is authorised by a judge of the High Court on the proposal of the Public Prosecutor of the High Public Prosecutor's Office or on the proposal of the European Delegated Prosecutor. Thus the agent can exercise their authority within and also outside of Czechia.	Code of Criminal Procedure Act No. 141/1961 Coll. Article 158e (paragraph 4)
What thresholds must be passed for the use of this tool?	If criminal proceedings are being conducted for the crime for which the law provides imprisonment for a term of at least eight years the tool is applicable.	Code of Criminal Procedure Act No. 141/1961 Coll. Article 158e (paragraph 1)
What types of stakeholder are involved in the implementation of this tool?	Use of an agent is authorised on the proposal of public prosecutor from the high public prosecutor's office by the high court judge in whose district the state prosecutor submitting the	Code of Criminal Procedure Act No. 141/1961 Coll. Article 158e (paragraph 4)

Relevant items	Provisions	Sources used
	proposal. The authorisation must state the purpose of agents use and the period for which the agent will be used, and data enabling identification of the agent. The period of authorisation can be extended on the basis of a new motion containing evaluation of the agent's activities to date, and may be repeatedly extended.	
Which LEAs can use this tool?	An agent is an officer of the Czech Police Forces or of General Inspection of Security Forces carrying out tasks assigned, by the police authority, usually involving concealment of the actual purpose of his/her activity.	Code of Criminal Procedure Act No. 141/1961 Coll. Article 158e (paragraph 2)
What are the rules to be followed for the implementation of this tool?	Use of an agent is authorised on the proposal of public prosecutor from the high public prosecutor's office by the high court judge in whose district the state prosecutor submitting the proposal. In other circumstances European Public Prosecutor can also request use of Agent. High court judge decided upon merits.	Code of Criminal Procedure Act No. 141/1961 Coll. Article 158e (paragraph 4)
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Particular law does not include any specific additional protection. All actions by the Police Forces can be addressed and scrutinised by the General Inspectorate of Security Forces (GIBS), or by the Court.	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Authorisation lies within the proposal of public prosecutor from the high public prosecutor's office by the high court judge in whose district the state prosecutor submitting the proposal. High court judge then decides upon merits.	Code of Criminal Procedure Act No. 141/1961 Coll. Article 158e (paragraph 4)
What ongoing supervision is required for the use of this tool?	National Legislation does not stipulate any specific ongoing supervision over this tool. Internal regulations and procedures are restricted for the personal of the respective units and are not publicly available	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	Act on Police Force of Czechia 273/2008 Coll. Article 73.	https://www.zakonyprolidi.cz/cs/2008-273
Specific range of application of the tool	No range applicable in this particular tool. All natural persons can be informants. The law does not specify any particular group of persons.	
How is the tool defined?	An informant means any natural person, which provides the police with information and services, in such way that his/her collaboration with the police is kept by confidence.	Act on Police Force of Czechia 273/2008 Coll. Article 73 (paragraph 1)
For what types of crime can the tool be used?	An informant means any natural person, which provides the police with information and services, in such way that his/her collaboration with the police is kept by confidence. There is no specification on which of the crimes can the Informants be used.	Act on Police Force of Czechia 273/2008 Coll. Article 73 (paragraph 1)
Does national law allow this tool to be used in cross-border cases?	Detailed rules for the implementation of the tool are restricted for Personnel of the respective units and are not publicly available.	
What thresholds must be passed for the use of this tool?	Due no specification of crimes are listed in the National law provisions, there are no thresholds mentioned in respect of imprisonment terms. No thresholds are available.	
What types of stakeholder are involved in the implementation of this tool?	National Legislation does not stipulate any specific stakeholders over this tool. Internal regulations and procedures are restricted for the personnel of the respective units and are not publicly available	
Which LEAs can use this tool?	The conditions for the use of informants are discretion of the Police of Czechia.	Act on Police Force of Czechia 273/2008 Coll. Article 73
What are the rules to be followed for the implementation of this tool?	National Legislation does not offer any information over this tool. Internal regulations and procedures are restricted for the personnel of the respective units and are not publicly available	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Particular law does not include any specific additional protection. All actions by the Police Forces can be addressed and scrutinised by the General Inspectorate of Security Forces (GIBS), or by the Court.	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	National Legislation does not stipulate any specific information on authorisation over this tool. Internal regulations and procedures are restricted for the personnel of the respective units and are not publicly available.	
What ongoing supervision is required for the use of this tool?	National Legislation does not stipulate any specific ongoing supervision over this tool. Internal regulations and procedures are restricted for the personal of the respective units and are not publicly available.	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	

Relevant items	Provisions	Sources used
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Pretended Transfer		
Relevant documents (legal and non-legal) that define the functioning of the tool	Code of Criminal Procedure Act No. 141/1961 Coll., Article 158b ; 158c.	https://www.zakonyprolidi.cz/cs/1961-141
How is the tool defined?	Pretended transfer means the simulation of purchase, sale or any other method of transfer object of which a special permit is necessary, the possession of which is impermissible, that originates from a criminal offence, or that is intended (designated, determined) for committing a criminal offence.	Code of Criminal Procedure Act No. 141/1961 Coll. Article 158c (paragraph 1)
For what types of crime can the tool be used?	There are no limitations in listed crimes for what this tool can be used.	Code of Criminal Procedure Act No. 141/1961 Coll. Article 158c
Does national law allow this tool to be used in cross-border cases?	Unless otherwise specified, the police authority, if authorised to do so by the relevant Minister. In the case of the department of the Office for Foreign Relations and Information, its director, authorised to use operational investigative means in proceedings on an intentional criminal offense, which means pretended transfer.	Code of Criminal Procedure Act No. 141/1961 Coll. Article 158b (paragraph1)
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	A pretended transfer can only be made with the written permission of the public prosecutor. If the matter cannot be postponed, the pretended transfer can be exercised without permission. However, the Police Forces is obliged to apply for a permit immediately afterwards, and if it is not granted within 48 hours, Police Forces are obliged to stop the pretended transfer and not use the information it has gathered in this regard.	Code of Criminal Procedure Act No. 141/1961 Coll. Article 158c (paragraph 2 & 3)
Which LEAs can use this tool?	Pretended transfer tool can be based on permission from the public prosecutor and is exercised by the Police Forces and General Inspection of Security Forces.	Code of Criminal Procedure Act No. 141/1961 Coll. Article 158c (paragraph 2 & 3)
What are the rules to be followed for the implementation of this tool?	National Legislation does not offer any rules to be followed over this tool. Internal regulations and procedures are restricted for the personnel of the respective units and are not publicly available	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Particular law does not include any specific additional protection. All actions by the Police Forces can be addressed and scrutinised by the General Inspectorate of Security Forces (GIBS), or by the Court.	
What authorisation is needed for the use of this tool?(e.g. senior police officer, prosecutor, judge, other)	A pretended transfer can only be made with the written permission of the public prosecutor. If the matter cannot be postponed, the pretended transfer can be exercised without permission. However, the Police Forces is obliged to apply for a permit immediately afterwards, and if it is not granted within 48 hours, Police Forces are obliged to stop the pretended transfer and not use the information it has gathered in this regard.	Code of Criminal Procedure Act No. 141/1961 Coll. Article 158c (paragraph 2 & 3)
What ongoing supervision is required for the use of this tool?	National Legislation does not stipulate any specific ongoing supervision over this tool. Internal regulations and procedures are restricted for the personal of the respective units and are not publicly available.	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	

Source: Author's own elaboration

Denmark

Table 24 – Overview of national rules on investigative tools - Denmark

Relevant items	Provisions	Sources used
Controlled Delivery		
Relevant documents (legal and non-legal) that define the functioning of the tool	Administration of Justice Act	https://www.legislationline.org/download/id/5372/file/DENMARK_ADMINISTRATIO_N_of_justice_act-2008_en-OK.pdf

Relevant items	Provisions	Sources used
How is the tool defined?	"Controlled delivery" means that the police are aware that one will be imported quantity of narcotics but fails to intervene, e.g. at the border crossing and instead follow the transport into the country in order to first strike at a convenient time where it is evidentially possible to hit as large a part of the organisation as possible.	Chapter 3, 3.1, page 127 para 5. https://translate.googleusercontent.com/translate_f
For what types of crime can the tool be used?	International drug crime.	Chapter 3, 3.1, page 126, para 1. https://translate.googleusercontent.com/translate_f
Does national law allow this tool to be used in cross-border cases?	The national law (administration justice law and criminal law etc.) does not specify this information. But Denmark is part of Schengen convention hence all rules are applicable to Denmark agreement. Article 73 (1) of Schengen acquis states that - The Contracting Parties undertake, in accordance with their constitutions and their national legal systems, to adopt measures to allow controlled deliveries to be made in the context of the illicit trafficking in narcotic drugs and psychotropic substances.	Article 73 (1), Schengen Acquis. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922(02):EN:HTML
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	The police department and prosecution department.	Chapter 10, § 104 of administration justice act. http://www.socialjura.dk/content-storage/love/love/retsplejelov-uddrag/#c49293
Which LEAs can use this tool?	LEAs.	Chapter 10, § 104 of administration justice act. http://www.socialjura.dk/content-storage/love/love/retsplejelov-uddrag/#c49293
What are the rules to be followed for the implementation of this tool?	National laws does not say anything about 'Controlled Delivery'. But, Denmark is the member of Schengen Acquis, hence, the following rules can be applied i.e. each Contracting Party may send the request to other Contracting Party for any information which may be important in helping in combat future crime and prevent offences against or threats to public policy and public security. 1. The Contracting Parties may conclude bilateral agreements providing for the secondment, for a specified or unspecified period, of liaison officers from one Contracting Party to the police authorities of another Contracting Party. 2. The secondment of liaison officers for a specified or unspecified period is intended to further and accelerate cooperation between the Contracting Parties, particularly by providing assistance: a) In the form of the exchange of information for the purposes of combating crime by means of both prevention and law enforcement. b) In executing requests for mutual police and judicial assistance in criminal matters. c) With the tasks carried out by the authorities responsible for external border surveillance.	- Article 46 (1). - Article 47 (1), (2), a,b,c. Schengen Acquis https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922(02):EN:HTML
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	No safeguard information is available in national laws, because this tool is NOT defined in national law. Whereas, EU also echoes that "Controlled deliveries are seen as narrower in their scope, as the primary focus and cause of action is the illicit commodity".	Section 7.10.9, page 289- the legal investigation tools. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/20150312_1_amoc_report_020315_0_220_part_2_en.pdf
What authorisation is needed for the use of this tool?	Please refer to the analysis above.	
What ongoing supervision is required for the use of this tool?	Please refer to the analysis above.	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Data available on the number of times this tool has been used for SOC cases	N/A	
Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	Schengen Convention	https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922(02):EN:HTML
How is the tool defined?	- There is no specific national law on hot pursuit in Denmark. Since the Convention implementing the Schengen Agreement (Schengen Convention) applies to Denmark, Art. 41 Schengen Convention is the basic relevant law. - Additionally, bilateral (for Germany and Sweden) agreements exist for interstate police cooperation, containing rules on hot pursuit. Those rules are mainly specifying Art. 41 Schengen Convention. All of the agreements are subject to cross-border police cooperation.	- Schengen Convention: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A42000A0922%2802%29 - Agreement with Germany: https://www.ris.bka.gv.at/Ergebnis.wxe?Abfrage=BgbAuth&Bgbnummer=210/2005&SucheNachTeil3=True
For what types of crime can the tool be used?	There is no specific national law on which crime hot pursuit should be carried out in Denmark. Since the Convention implementing the Schengen Agreement (Schengen Convention) applies to Denmark, Art. 41- 4 (a) of Schengen Convention states the following crimes to be considered: murder, manslaughter, rape, arson, forgery of money, aggravated burglary and robbery and receiving stolen goods, extortion, kidnapping and hostage taking, trafficking in human beings, illicit trafficking in narcotic drugs and psychotropic substances, breach of the laws on arms and explosives, wilful damage through the use of explosives, illicit transportation of toxic and	- Article 41-4 (a) Schengen convention https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922(02):EN:HTML - EJN also echoes the same - https://www.ejn-crimjust.europa.eu/ejn/EJN_FichesBelgesResult/EN/802/260/-1

Relevant items	Provisions	Sources used
	hazardous waste, failure to stop and give particulars after an accident which has resulted in death or serious injury.	
Does national law allow this tool to be used in cross-border cases?	As stated above, Denmark does not have any specific law about hot pursuit. But as per European Judicial Network (EJN), there exists a special agreement in between Denmark, Sweden and Germany allows to use this tool in cross-border cases.	Point 2 of EJN Denmark case- https://www.ejn-crimjust.europa.eu/ejn/EJN_FichesBelgesResult/EN/802/260/-1
What thresholds must be passed for the use of this tool?	Denmark does not have any rules about hot pursuit. But as per the European Judicial Network (of which Denmark is a member) states that, Only when pursuing a person suspected of serious crime, may foreign police conduct cross-border hot pursuit. Within the ambit of serious crime falls, murder, manslaughter, severe sexual crimes, extortion, extensive theft, and extensive economical crime.	Point 6 (a) of EJN Denmark case- https://www.ejn-crimjust.europa.eu/ejn/EJN_FichesBelgesResult/EN/802/260/-1
What types of stakeholder are involved in the implementation of this tool?	National Commissioner Office, local police and prosecutor.	Point 3 of EJN Denmark case- https://www.ejn-crimjust.europa.eu/ejn/EJN_FichesBelgesResult/EN/802/260/-1
Which LEAs can use this tool?	Due to the lack of national law, Denmark can follow the European Judicial Network's suggestions which says - if other country's officer is entering in the Denmark, then the request has to be submitted to National Commission's office and then respective prosecutor can give decision on it. After the decision, the National Commission office can order local police to execute the task.	Point 2 of EJN Denmark case- https://www.ejn-crimjust.europa.eu/ejn/EJN_FichesBelgesResult/EN/802/260/-1
What are the rules to be followed for the implementation of this tool?	Denmark does not have any rules about hot pursuit. But as per the European Judicial Network (of which Denmark is a member) states that, "1) As a general rule, German and Swedish police officers may only move up to a distance of 25 km from the border of Denmark. 2) Any foreign police personnel must adhere to national Danish law when operating on Danish territory. 3) Foreign police personnel must be clearly recognizable, e.g. through uniforms, marked cars, armbands or the like". 4) Foreign police may not access places which are not open to the public. 5) Service arms may be carried by foreign police during a cross-border observation. 6) After a cross-border hot pursuit the foreign police officers must personally be available to the local police authorities with the purpose of making an adequate report on the operation.	Point 6 (a) of EJN Denmark case- https://www.ejn-crimjust.europa.eu/ejn/EJN_FichesBelgesResult/EN/802/260/-1
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Being a member of Schengen convention, the followings are applicable: - The pursuing officers must comply with the provisions of convention and with the law of country in whose territory they are operating; they must obey the instructions issued by the competent local authorities. - Pursuit shall be solely over land borders. - Entry into private homes and places not accessible to the public shall be prohibited. - The pursuing officers shall be easily identifiable, either by their uniform, by means of an armband or by accessories fitted to their vehicles; the use of civilian clothes combined with the use of unmarked vehicles without the aforementioned identification is prohibited; e) the pursuing officers must at all times be able to prove that they are acting in an official capacity. - The pursuing officers may carry their service weapons; their use shall be prohibited save in cases of legitimate self-defence. - Once the pursued person has been apprehended for the purpose of being brought before the competent local authorities that person may only be subjected to a security search; handcuffs may be used during the transfer; objects carried by the pursued person may be seized. - After each operation the pursuing officers shall appear before the competent local authorities of the Contracting Party in whose territory they were operating and shall report on their mission; at the request of those authorities, they shall remain at their disposal until the circumstances surrounding their action have been sufficiently clarified; this condition shall apply even where the hot pursuit has not resulted in the arrest of the person pursued. - The authorities of the Contracting Party from which the pursuing officers have come shall, when requested by the authorities of the Contracting Party in whose territory the hot pursuit took place, assist the enquiry subsequent to the operation in which they took part, including judicial proceedings.	Art. 41, (5) - a, b ,c ,d ,e and f of Schengen convention. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922(02):EN:HTML
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	National Commissioner Office, local police and prosecutor.	Point 2 of EJN Denmark case- https://www.ejn-crimjust.europa.eu/ejn/EJN_FichesBelgesResult/EN/802/260/-1
Is there any national case law relating to the use of this tool in cross-border crime cases?	Usually, no authorisation is necessary, since it lies in the nature of the tool that it has to be used instantly without the need of authorisation processes.	Art 41 para 1. and para. 4 Schengen Convention
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Witness protection		

Relevant items	Provisions	Sources used
Relevant documents (legal and non-legal) that define the functioning of the tool	Administration of Justice Act.	https://www.legislationline.org/download/id/5372/file/DENMARK_ADMINISTRATIO_N_of_justice_act-2008_en-OK.pdf
How is the tool defined?	Everyone has a duty to testify before the court as a witness.	Chapter 18, § 168 of administration of justice act
For what types of crime can the tool be used?	There is no specific national law on which crime witness protection should be carried out in Denmark. Since the Convention implementing the Schengen Agreement (Schengen Convention) applies to Denmark, Art. 41- 4 (a) of Schengen Convention states the following crimes to be considered: murder, manslaughter, rape, arson, forgery of money, aggravated burglary and robbery and receiving stolen goods, extortion, kidnapping and hostage taking, trafficking in human beings, illicit trafficking in narcotic drugs and psychotropic substances, breach of the laws on arms and explosives, wilful damage through the use of explosives, illicit transportation of toxic and hazardous waste, failure to stop and give particulars after an accident which has resulted in death or serious injury.	- Article 41-4 (a) Schengen convention https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922(02):EN:HTML - EJN also echoes the same - https://www.ejn-crimjust.europa.eu/ejn/EJN_FichesBelgesResult/EN/802/260/-1
Does national law allow this tool to be used in cross-border cases?	As stated above, Denmark does not have any specific law about witness protection. But as per European Judicial Network (EJN), there exists a special agreement in between Denmark, Sweden and Germany allows to use this tool in cross-border cases.	Point 2 of EJN Denmark case- https://www.ejn-crimjust.europa.eu/ejn/EJN_FichesBelgesResult/EN/802/260/-1
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	LEAs	Art 171 (2) Administration of justice act
Which LEAs can use this tool?	LEAs and police department	Art. 856 Administration of justice act
What are the rules to be followed for the implementation of this tool?	The prosecution does not have to inform the court about their initiatives in this regard. Police reports do not have to contain names of witnesses but can say 'a source known to police' instead. The prosecution can request the court to accept these anonymous testimonies as grounds to proceed with the court hearing. If the court request that the witness testifies in court there are rules that regulate 'closing of doors', names can be removed from the publicly accessible witness lists, the names can be withheld from the defense.	Art. 856 Administration of justice act
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Witnesses also have a 'qualified penal protection' where violence and threats against witnesses has a maximum sanction of eight years imprisonment	Penal code, Section 123
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Besides from the general right to guidance, an alleged victim also has a specific right to guidance on appointment of counsel, on the content of the rules regarding witness exclusion, on the possibility of pursuing a civil claim during the criminal case, and to Appoint a Contact Person for the Victim on the possibility of receiving compensation from the state, on the Police's and the Prosecution's Duty to Provide Guidance and Inform Victims in Criminal Cases and to Appoint a Contact Person for the Victim, and on the possibility of receiving victim counselling, and inform Victims in Criminal Cases and to Appoint a Contact Person for the Victim.	- Section 741 b(1) of the Administration of Justice Act - Section 753 of the Administration of Justice Act - Section 1(1)(2) of the Executive Order on the Police's and the Prosecution's Duty to Provide Guidance and Inform Victims in Criminal Cases - Section 1(1)(3) of the Executive Order on the Police's and the Prosecution's Duty to Provide Guidance and Inform Victims in Criminal Cases - Section 1(1)(4) of the Executive Order on the Police's and the Prosecution's Duty to Provide Guidance
What ongoing supervision is required for the use of this tool?	When police receives a complaint then police must evaluate whether there is a reasonable suspicion that an offence that can be prosecuted by the public prosecutor has occurred. If that is the case, the police must initiate an investigation into the alleged offence. However, if the police do not find that there are sufficient grounds for initiating an investigation, the police dismiss the complaint.	- Section 742(2) of the Administration of Justice Act - Section 749(1) of the Administration of Justice Act
Is there any national case law relating to the use of this tool in cross-border crime cases?	There is no supervision is required in this tool except protection to the witness in organised or serious crime. The use of anonymous witnesses builds on an earlier decision to allow courts to withhold witness' name, occupation, and address described in administration act implemented with Act no. 381 of June 6, 2002. With the amendment from 2011 to , courts can decide that the defendant must leave the courtroom while a witness gives testimony, if this is required in order to get a full testimony.	1) Administration of Justice Act, Section 856, stk. 2 - Section 848 of the Administration of Justice Act
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Surveillance		
Relevant documents (legal and non-legal) that define the functioning of the tool	- TV surveillance act - Administration of justice act	http://www.socialjura.dk/love/tv-overvaagningslov/menu/all/love/ https://www.legislationline.org/download/id/5372/file/DENMARK_ADMINISTRATIO_N_of_justice_act-2008_en-OK.pdf
Specific range of application of the tool	CCTV is used widely for combating crime.	TV surveillance act § 2, 5 (1) http://www.socialjura.dk/love/tv-overvaagningslov/menu/all/love/
How is the tool defined?	TV surveillance means continuous or regularly repeated personal surveillance by means of a remote-controlled or automatically operating television camera, camera or similar apparatus. The	TV surveillance act § 1, PCS. 2. http://www.socialjura.dk/love/tv-overvaagningslov/menu/all/love/

Relevant items	Provisions	Sources used
	rules of the Act on television surveillance apply correspondingly to the installation of such a device for the purpose of surveillance.	
For what types of crime can the tool be used?	In Danish's national law (penal code, administration of justice act) 'Surveillance' is poorly defined. But being the member of Schengen convention, surveillance can be defined as "Officers of one of the Contracting Parties who, as part of a criminal investigation, are keeping under surveillance in their country a person who is presumed to have participated in an extraditable criminal offence shall be authorised to continue their surveillance in the territory of another Contracting Party where the latter has authorised cross-border surveillance in response to a request for assistance made in advance"	Article 40 (1), of Schengen Convention. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922(02):EN:HTML
Does national law allow this tool to be used in cross-border cases?	The surveillance may only be carried out where one of the following criminal offences is involved: murder, manslaughter, rape, arson, forgery of money, aggravated burglary and robbery and receiving stolen goods, extortion, kidnapping and hostage taking, trafficking in human beings, illicit trafficking in narcotic drugs and psychotropic substances, breach of the laws on arms and explosives, wilful damage through the use of explosives, illicit transportation of toxic and hazardous waste.	Article 40 (7), of Schengen Convention. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922(02):EN:HTML
What thresholds must be passed for the use of this tool?	National law does not specify but being a member of Schengen convention hence this tool can be used in cross-border cases.	Article 40 (1), of Schengen Convention. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922(02):EN:HTML
What types of stakeholder are involved in the implementation of this tool?	If person is involved in any of the crime mentioned above then procedure mentioned above has to be carried out. No information found on term of imprisonment.	Article 40 (3), a, b, c, d, e, f, g, h of Schengen convention
Which LEAs can use this tool?	LEAs.	Administration of Justice Act, Section 856, stk. 2.
What are the rules to be followed for the implementation of this tool?	National Investigation Centre (NEC) - An investigative centre which comprises a number of regional and specialised task forces: namely the East, West, Burglary and Pusher Street task forces. National Police - The National Police coordinates the activities of various investigative bodies (with the exception of the SØIK and SKAT). State Attorney of International Economic Crime (SØIK) Internal Revenue Service (SØK and SKAT). SØK, SØIK, Finanstilsynet and SKAT work closely together with the NEC on the economic aspects of organised crime cases. These agencies work together on specific cases, but share information on a regular basis.	Page 543, table https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/20150312_1_amoc_report_020315_0_220_part_2_en.pdf
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	The national law does not comment on this tool. However, Schengen Convention says that the surveillance can be carried out on the following conditions: a) The officers carrying out the surveillance must comply with the provisions of this Article and with the law of the Contracting Party in whose territory they are operating; they must obey the instructions of the competent local authorities. b) Except in the situations the officers shall, during the surveillance, carry a document certifying that authorisation has been granted. c) The officers carrying out the surveillance must at all times be able to prove that they are acting in an official capacity. d) The officers carrying out the surveillance may carry their service weapons during the surveillance save where specifically otherwise decided by the requested Party; their use shall be prohibited save in cases of legitimate self-defence. e) Entry into private homes and places not accessible to the public shall be prohibited. f) The officers carrying out the surveillance may neither challenge nor arrest the person under surveillance. g) All operations shall be the subject of a report to the authorities of the Contracting Party in whose territory they took place; the officers carrying out the surveillance may be required to appear in person. h) The authorities of the Contracting Party from which the surveillance officers have come shall, when requested by the authorities of the Contracting Party in whose territory the surveillance took place, assist the enquiry subsequent to the operation in which they took part, including judicial proceedings.	Article 40 (3), a, b, c, d, e, f, g, h of Schengen convention
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	National law does not say anything about this tool but according to Schengen convention «The request for assistance referred to in the first subparagraph must be sent to an authority designated by each of the Contracting Parties and empowered to grant or to pass on the requested authorisation».	Article 40 (1) para 2,, of Schengen Convention. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922(02):EN:HTML
Is there any national case law relating to the use of this tool in cross-border crime cases?	Due to lack of use of this tool in national laws, Schengen convention says that - for particularly urgent reasons, prior authorisation cannot be requested from the other Contracting Party, the officers carrying out the surveillance shall be authorised to continue beyond the border the surveillance of a person presumed to have committed criminal offences the following conditions are met: a) The authority of the Contracting Party designated in whose territory the surveillance is to be continued, must be notified immediately, during the surveillance, that the border has been crossed.	Article 40-2 a and b of Schengen Convention. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922(02):EN:HTML

Relevant items	Provisions	Sources used
	b) A request for assistance submitted and outlining the grounds for crossing the border without prior authorisation shall be submitted immediately. c) Surveillance shall cease as soon as the Contracting Party in whose territory it is taking place so requests, following the notification referred to in (a) or the request referred to in (b) or, where authorisation has not been obtained, five hours after the border was crossed.	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Undercover / covert operations		
Relevant documents (legal and non-legal) that define the functioning of the tool	Administration of Justice Act	https://www.legislationline.org/download/id/5372/file/DENMARK ADMINISTRATIO N of justice act-2008 en-OK.pdf
How is the tool defined?	This tool is not properly defined in national law but administration of justice act says that "At the police questioning of a person who has not been charged, the provisions of §§ 173, para. 1, 182 and 184, para. 1 and 2, corresponding application"	Chapter 68, § 753 of Administration of justice act
For what types of crime can the tool be used?	Being a member of Schengen convention, this tool is defined as 'Covert investigation' is the term commonly used in European legislation to refer to the 'use of undercover officers'.	Convention on mutual assistance and cooperation between customs administrations (Naples II). See (as of 3 February 2015: http://europa.eu/legislation_summaries/customs/l33051_en.htm
Does national law allow this tool to be used in cross-border cases?	Illicit drugs	Judicial Commission's recommendations in Parliamentary Report no. 1023/1984
What thresholds must be passed for the use of this tool?	No. However, it can be inferred that in Denmark, Surveillance and undercover tools were used together.	Sections 754a – 754e of Administration of justice act
What types of stakeholder are involved in the implementation of this tool?	No information found.	The previous stud also confirms that there is no information found on this topic
Which LEAs can use this tool?	LEAs.	Sections 754a – 754e of Administration of justice act
What are the rules to be followed for the implementation of this tool?	National Investigation Centre (NEC) - An investigative centre which comprises a number of regional and specialised task forces: namely the East, West, Burglary and Pusher Street task forces. National Police - The National Police coordinates the activities of various investigative bodies (with the exception of the SØIK and SKAT). State Attorney of International Economic Crime (SØIK) Internal Revenue Service (SØK and SKAT). SØK, SØIK, Finanstilsynet and SKAT work closely together with the NEC on the economic aspects of organised crime cases. These agencies work together on specific cases, but share information on a regular basis.	Page 543, table https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/20150312_1_amoc_report_020315_0_220_part_2_en.pdf
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	"Particularly well-founded suspicion" that a criminal act is about to take place in order to avoid provocation. Initiation of this tool requires a court order.	1) Section 754 a. 2) Section 754 c, and 3) Section 754 d of The Administration of Justice Act
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	In suspicions of future criminal activity, police can use this tool upon asking for permission from prosecutors.	Chapter 68, § 753 of Administration of justice act
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	Administration of Justice Act.	https://www.legislationline.org/download/id/5372/file/DENMARK ADMINISTRATIO N of justice act-2008 en-OK.pdf
Specific range of application of the tool	The measures may only be carried out by police officers and police officers with special investigative qualifications. However, civilians may, in agreement with the police, provide assistance to commit or continue the offense under investigation when the assistance provided in relation to the offense.	Administration of justice act, § 754 b, PCS.2. http://www.socialjura.dk/content-storage/love/love/retsplejelov-uddrag/#c70038
How is the tool defined?	"The purpose of the police's co-operation with informants is to prevent and fight crime by the police receiving information about persons in the criminal environment from the informant. Much of the information provided by informants relates to planned or committed crimes which are either already under investigation or which give rise to the police initiating an investigation.	Parliamentary report 1023 (1984), p. 159-160).

Relevant items	Provisions	Sources used
For what types of crime can the tool be used?	Narcotic drugs.	Police intervention in the message secret and use of agent, Report No 10231984 Ministry of Justice's Criminal Justice Committee, page 128 para 5. https://www.elov.dk/media/betaenkninger/Politiets_indgreb_i_meddelelseshemme_ligheden_og_anvendelse_af_agenter.pdf
Does national law allow this tool to be used in cross-border cases?	No. The legislation does not contain any provisions on police use of agents in the context of the investigation of offenses parts. There are also no administrative regulations set such rules. However, in connection with the use of the establishment of agents internally set certain guidelines, but it must be emphasised that these are only guidelines which are used in the individual police district, and these guidelines has not resulted in a central approach being drawn.	Police intervention in the message secret and use of agent, Report No 10231984 Ministry of Justice's Criminal Justice Committee, page 129, para 1 section 3.2 https://www.elov.dk/media/betaenkninger/Politiets_indgreb_i_meddelelseshemme_ligheden_og_anvendelse_af_agenter.pdf
What thresholds must be passed for the use of this tool?	N/A	The previous study also confirms that there is no information found on this topic.
What types of stakeholder are involved in the implementation of this tool?	Chief of the National Police and the Association of Chiefs of Police that to be kept in connection with the Police Investigation Support Database (PED).	Draft notice pkt. 6.3 from Parliamentary report 1023 (1984), p. 159-160. https://www.datatilsynet.dk/tilsyn-og-afgoerelser/historiske-afgoerelser/2005/mar/vedroerende-rigsadvokatens-retningslinier-vedroerende-meddelere
Which LEAs can use this tool?	LEAs.	
What are the rules to be followed for the implementation of this tool?	Investigation of criminal offenses is handled by the police.	Section 742 of the Code of Judicial Procedure
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	The National Commissioner of Police has access to the informant lists in all police districts.	
What ongoing supervision is required for the use of this tool?	N/A	The previous study also confirms that there is no information found on this topic.
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	

Source: Author's own elaboration

Estonia

Table 25 – Overview of national rules on investigative tools - Estonia

Relevant items	Provisions	Sources used
Controlled Delivery		
Relevant documents (legal and non-legal) that define the functioning of the tool	N/A	
How is the tool defined?	N/A	
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross-border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	

Relevant items	Provisions	Sources used
What authorisation is needed for the use of this tool?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Data available on the number of times this tool has been used for SOC cases	N/A	
Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	N/A	
How is the tool defined?	N/A	
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross-border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	Witness Protection Act.	This act is passed by Riigikogu, passed 15.06.2005, RT I 2005, 39, 307, entry into force 21.07.2005, https://www.riigiteataja.ee/en/eli/530122013001/consolide
How is the tool defined?	A person who may know facts relating to a subject of proof in a criminal case is under actual risk of falling subject to unlawful influence and the person consents to co-operate with the witness protection authority.	§ 6. Conditions for application of witness protection of Witness protection act. https://www.riigiteataja.ee/en/eli/530122013001/consolide
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross-border cases?	The witness protection authority (it is an authority formed under § 4 (1)) shall initiate witness protection procedures at the request of a foreign competent authority or an international organisation pursuant to international agreements entered into. In order to apply witness protection in the territory of the Republic of Estonia to a person protected by a foreign state or an international organisation, a separate agreement shall be entered into by the competent authorities with respect to each person protected by a foreign state or an international organisation.	§ 17 (1) Witness protection act. https://www.riigiteataja.ee/en/eli/530122013001/consolide
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	The Central Criminal Police organises witness protection. Other state and local government bodies and agencies and legal persons in public law are required to assist in witness protection within the limits of their competence.	§ 4. Witness protection authority of witness protection act

Relevant items	Provisions	Sources used
	- Supervision over witness protection shall be exercised by the Public Prosecutor's Office. - The Central Criminal Police organises international co-operation in witness protection with competent foreign agencies and international organisations pursuant to international agreements.	
Which LEAs can use this tool?	Witness protection is carried out by the Police and Border Guard Board.	§ 4 (1) Witness protection authority of witness protection act
What are the rules to be followed for the implementation of this tool?	- The witness protection procedure in respect of a person is initiated by a written order of the head of the witness protection authority or an official appointed by him or her, based on the following: - A reasoned written request of the person conducting proceedings in the corresponding criminal matter together with the written consent of the protected person. - A reasoned request of the person conducting the proceedings or an official exercising supervisory control over such official in case any of the circumstances specified in clause 5 (2) 2) of this Act occur. - In case the protected person or his or her family member or close relative is a person with restricted active legal capacity, the written consent of the legal representative or guardianship authority of such person is required for the initiation of the witness protection procedure. If possible, the person with restricted active legal capacity is asked for his or her opinion, taking into account the ability of the person to comprehend.	§ 9 (1), (2) Initiation of witness protection procedure in respect of person. Witness protection act. https://www.riigiteataja.ee/en/eli/530122013001/consolide
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	- In the course of the processing of an application for witness protection, the following shall be established and assessed: - Whether the evidence to be given by the protected person are necessary for the criminal proceedings and whether the evidence can be replaced with other evidence. - Whether the protected person has given true statements and whether he or she is ready to give true statements until the termination of the criminal proceedings. - The criminal record of the protected person, the obligations and restrictions imposed on the person under criminal or civil law. - The state of health of the protected person. - Unlawful influence on which the protected person may fall subject to. - Whether protection measures should also be used to protect the health and property of the family members or close relatives of the protected person. - Which protection measures during which time period should be applied and whether necessary resources are available for the application of such measures. - Whether the rights or legitimate interests of another person may be at risk if the protection measures are applied. - In order to ascertain the circumstances specified in subsection (1) of this section, the officials of the witness protection authority have the right to: - Have access to the existing surveillance and investigation material. - Question the persons conducting the proceedings concerned. - Question the protected persons. - Use the assistance of general practitioners, medical specialists and psychologists in order to assess the suitability of the protection measures to be applied and the personal characteristics of the protected person. - Make inquiries to agencies maintaining databases and registries. - Conduct surveillance activities in order to ascertain circumstances relating to the application of witness protection pursuant to the Surveillance Act. - The verification and analysis of the circumstances specified in subsection (1) of this section shall be made within thirty days as of the initiation of the witness protection procedure.	§ 10 (1), (2), and (3) Initiation of witness protection procedure in respect of person. Witness protection act. https://www.riigiteataja.ee/en/eli/530122013001/consolide
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	- The following protection measures are applied in witness protection: - Physical protection of the protected person and his or her property. - Provision of self-defence equipment for the protected person. - Provision of new telecommunications or telecommunication numbers for the protected person. - Provision of new registration marks for the means of transportation of the protected person. - Provision of new place of residence, workplace or place of studies for the protected person. - Secret relocation of the protected person to a safe area or locality. - Changing the appearances of the protected person through plastic surgery. - Creation of new identity for the protected person. - Other protection measures. - The protection measures listed in subsection (1) of this section may be applied either separately or in combination. - In applying witness protection measures, the witness protection authority has the right to conduct surveillance activities pursuant to the Surveillance Act.	§ 18 (1), (2), (3), (4). Witness protection measures. Witness protection act. https://www.riigiteataja.ee/en/eli/530122013001/consolide

Relevant items	Provisions	Sources used
	The documents necessary for the application of a witness protection measure specified in a witness protection agreement are issued and the necessary amendments in databases and registries are made, at a reasoned request of the head of the witness protection authority, by an administrative authority or a legal person into whose competence the issue of corresponding documents or making of such amendments falls.	
What ongoing supervision is required for the use of this tool?	- The Central Criminal Police organises witness protection. Other state and local government bodies and agencies and legal persons in public law are required to assist in witness protection within the limits of their competence. - Supervision over witness protection shall be exercised by the Public Prosecutor's Office. - The Central Criminal Police organises international co-operation in witness protection with competent foreign agencies and international organisations pursuant to international agreements	§ 4. Witness protection authority of witness protection act
Is there any national case law relating to the use of this tool in cross-border crime cases?	Supervision over witness protection shall be exercised by the Public Prosecutor's Office.	§ 4. Witness protection authority of witness protection act
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Surveillance		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Procedural Law	https://www.riiqiteataja.ee/akt/12749538?leiaKehtiv
Specific range of application of the tool	National Law does not mentioned any of audio-video activities, whereas it says 'whereabouts'.	§ 472. Cross-border surveillance. Criminal Procedure Law. https://www.riiqiteataja.ee/akt/12749538?leiaKehtiv
How is the tool defined?	Surveillance is the processing of personal data for the performance of a task provided by law with the aim of concealing the fact and content of data processing from the data subject.	§ 126 1 (1), Chapter 3 of Criminal Procedure Law. https://www.riiqiteataja.ee/akt/12749538?leiaKehtiv
For what types of crime can the tool be used?	Cross-border crimes, organised crimes. In case of cross-border cases, murder, killing, a serious sexual offense etc (the list contains 20 items).	Section 3 § 472 (4) 1 to 19. Criminal procedure law. https://www.riiqiteataja.ee/akt/12749538?leiaKehtiv
Does national law allow this tool to be used in cross-border cases?	Submission of a request for cross-border surveillance from another Schengen Member State is permitted in pre-trial proceedings concerning the criminal offences.	subsection -1262 (2) of Criminal Procedure Law. https://www.riiqiteataja.ee/akt/12749538?leiaKehtiv
What thresholds must be passed for the use of this tool?	- A person in respect of whom there are reasonable grounds to believe that he or she commits a criminal offense specified in subsection (2) of criminal law. - Against a person who has been declared wanted. - To a person who owns or possesses property which is the object of confiscation proceedings. - To a person who is a suspect in criminal proceedings or in respect of whom there are reasonable grounds to believe that he or she committed or is committing the specified criminal offense.	§ 126-2 (3) (1,2,3), Chapter 3 of Criminal Procedure Law. https://www.riiqiteataja.ee/akt/12749538?leiaKehtiv
What types of stakeholder are involved in the implementation of this tool?	- Need to collect information on preparation for crime. - Compliance with a ruling declaring a person wanted. - The need to collect information in confiscation proceedings pursuant to 16 1 of Criminal procedure code. - The need to collect information on the criminal offense in criminal proceedings.	§ 126-2 (1) 1,2,3,4. Chapter 3 of Criminal Procedure Law. https://www.riiqiteataja.ee/akt/12749538?leiaKehtiv
Which LEAs can use this tool?	In case of cross-border surveillance, in connection with pre-trial proceedings for extradition, if the person is being monitored on suspicion of criminal offenses or in order to facilitate the identification or whereabouts of a suspect, surveillance may continue in the territory of another State party to the Schengen Convention of 19 June 1990. The Schengen Agreement of 14 June 1985 on the gradual abolition of checks at common borders, provided that the latter has authorised cross-border surveillance on the basis of a prior and reasoned request. Additional conditions may be attached to the permit.	Section 3 § 472 (1) of criminal procedure law. https://www.riiqiteataja.ee/akt/12749538?leiaKehtiv
What are the rules to be followed for the implementation of this tool?	The Police and Border Guard Board, the Security Police Board, the Tax and Customs Board, the Military Police and the Prisons Department of the Ministry of Justice and prisons may perform surveillance.	§ 126 2 (1), Chapter 3 of Criminal Procedure Law. https://www.riiqiteataja.ee/akt/12749538?leiaKehtiv
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	The Police and Border Guard Board, the Security Police Board, the Tax and Customs Board, the Military Police and the Prisons Department of the Ministry of Justice and prisons may perform surveillance.	§ 126 2 (1), Chapter 3 of Criminal Procedure Law. https://www.riiqiteataja.ee/akt/12749538?leiaKehtiv
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	In case of cross-border surveillance, the Public Prosecutor's Office is competent to submit an application for cross-border surveillance to another Schengen Member State; in urgent cases, the application may be submitted by the district prosecutor's office. The Public Prosecutor's Office	Section 3 § 472 (2) of criminal procedure law. https://www.riiqiteataja.ee/akt/12749538?leiaKehtiv

Relevant items	Provisions	Sources used
	shall issue a permit for the satisfaction of an application for cross-border surveillance submitted to Estonia.	
What ongoing supervision is required for the use of this tool?	1) Surveillance acts shall not endanger the life and health of a person, unreasonably endanger property and the environment or unreasonably infringe other personal rights. 2) Surveillance acts shall be performed directly through the agencies specified in subsection 126 2 (1) of this Code as well as agencies administered by them and agencies, subdivisions and employees authorised to perform surveillance acts, as well as through police agents, undercover agents and persons involved in secret co-operation.	§ 126 1 (3 and 5), Chapter 3 of Criminal Procedure Law. https://www.riigiteataja.ee/akt/12749538?leiaKehtiv
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	The Prosecutor's Office shall issue a permit for covert surveillance of a person, thing or locality, covert collection of reference material and performance of preliminary investigations and covert examination or replacement of a thing for up to two months. The Prosecutor's Office may extend the term of the permit by up to two months.	§ 126-5 (1), Chapter 3 of Criminal Procedure Law. https://www.riigiteataja.ee/akt/12749538?leiaKehtiv
Undercover / covert operations		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Procedural Law	https://www.riigiteataja.ee/akt/12749538?leiaKehtiv
How is the tool defined?	Covert surveillance is the processing of personal data for the performance of a task provided by law with the aim of concealing the fact and content of data processing from the data subject.	§ 126-1 (1), Chapter 3 of Criminal Procedure Law. https://www.riigiteataja.ee/akt/12749538?leiaKehtiv
For what types of crime can the tool be used?	A police agent is a person who, using a changed identity, collects information on the basis specified in clauses 126 2 (1) 1), 3) or 4) of criminal procedure code.	§ 126-9 (1), Chapter 3 of Criminal Procedure Law. [RT I, 06.01.2016, 5 - entry into force. 01.07.2016]. https://www.riigiteataja.ee/akt/12749538?leiaKehtiv
Does national law allow this tool to be used in cross-border cases?	Cross-border crimes, organised crimes. In case of cross-border cases, murder, killing, a serious sexual offense etc (the list contains 20 items).	Section 3 § 472 (4) 1 to 19. Criminal procedure law. https://www.riigiteataja.ee/akt/12749538?leiaKehtiv
What thresholds must be passed for the use of this tool?	There is no specific mentioned in national law. However, it depends upon the severity of the crime. In such cases prosecutor office may give the permission.	§ 126-2 (1), Chapter 3 of Criminal Procedure Law. https://www.riigiteataja.ee/akt/12749538?leiaKehtiv
What types of stakeholder are involved in the implementation of this tool?	- Covertly inspect a postal item. - Secretly view or listen to information. - Use a police agent.	§ 126-3 (2) 1,2, and 3. Chapter 3 of Criminal Procedure Law. https://www.riigiteataja.ee/akt/12749538?leiaKehtiv
Which LEAs can use this tool?	The Police and Border Guard Board, the Security Police Board, the Tax and Customs Board, the Military Police and the Prisons Department of the Ministry of Justice and prisons may perform surveillance.	§ 126 2 (1), Chapter 3 of Criminal Procedure Law. https://www.riigiteataja.ee/akt/12749538?leiaKehtiv
What are the rules to be followed for the implementation of this tool?	Judiciary, Prosecutor and police. In all cases the authorisation from Prosecutor is the must.	Section 3 § 472 (2) of criminal procedure law. https://www.riigiteataja.ee/akt/12749538?leiaKehtiv
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	1) The use of a police agent is granted for up to six months and this term may be extended by up to six months at a time. 2) A police agent has all the obligations of an official of a surveillance agency in so far as the obligations do not require disclosure of the false identity, 3) The statements of a police agent are used as evidence pursuant to the provisions of this Code concerning witnesses. (4) Based on an order of a Prosecutor's Office, the fact of using a police agent or the identity of a police agent shall also remain confidential after completion of surveillance activities if disclosure may endanger the life or health, honour and good name or property of the police agent or the persons connected with him or her or his or her further activities as a police agent.	§ 126-9 (2) 3,4,5, Chapter 3 of Criminal Procedure Law. https://www.riigiteataja.ee/akt/12749538?leiaKehtiv
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	1) Surveillance acts shall not endanger the life and health of a person, unreasonably endanger property and the environment or unreasonably infringe other personal rights. 2) Surveillance acts shall be performed directly through the agencies specified in subsection 126 2 (1) of this Code as well as agencies administered by them and agencies, subdivisions and employees authorised to perform surveillance acts, as well as through police agents, undercover agents and persons involved in secret co-operation.	§ 126 1 (3 and 5), Chapter 3 of Criminal Procedure Law. https://www.riigiteataja.ee/akt/12749538?leiaKehtiv
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	The Prosecutor's Office shall issue written permission for the use of a police agent.	§ 126-9 (2), Chapter 3 of Criminal Procedure Law. https://www.riigiteataja.ee/akt/12749538?leiaKehtiv
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	There is no specific mentioned in national law.	§ 126-2 (1), Chapter 3 of Criminal Procedure Law. https://www.riigiteataja.ee/akt/12749538?leiaKehtiv
Use of informants		

Relevant items	Provisions	Sources used
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Procedural Law.	https://www.riigiteataja.ee/akt/12749538?leiaKehtiv
Specific range of application of the tool	National Law does not mentioned any of audio-video activities, whereas it says 'whereabouts'.	§ 472. Cross-border surveillance. Criminal Procedure Law. https://www.riigiteataja.ee/akt/12749538?leiaKehtiv
How is the tool defined?	Use of informants is allowed, but there is no distinct regulation for the use of informants.	This findings matches with the previous study
For what types of crime can the tool be used?	Cross-border crimes, organised crimes. In case of cross-border cases, murder, killing, a serious sexual offense etc (the list contains 20 items).	Section 3 § 472 (4) 1 to 19.Criminal procedure law. https://www.riigiteataja.ee/akt/12749538?leiaKehtiv
Does national law allow this tool to be used in cross-border cases?	Submission of a request for cross-border surveillance from another Schengen Member State is permitted in pre-trial proceedings concerning the criminal offences.	subsection -1262 (2) of Criminal Procedure Law. https://www.riigiteataja.ee/akt/12749538?leiaKehtiv
What thresholds must be passed for the use of this tool?	- Against person in respect of whom there are reasonable grounds to believe that he or she commits a criminal offense specified in subsection (2) of this section. - Against a person who has been declared wanted. - To a person who owns or possesses property which is the object of confiscation proceedings. - To a person who is a suspect in criminal proceedings or in respect of whom there are reasonable grounds to believe that he or she committed or is committing the specified criminal offense.	§ 126-2 (3) (1,2,3), Chapter 3 of Criminal Procedure Law. https://www.riigiteataja.ee/akt/12749538?leiaKehtiv
What types of stakeholder are involved in the implementation of this tool?	The Police and Border Guard Board, the Security Police Board, the Tax and Customs Board, the Military Police and the Prisons Department of the Ministry of Justice and prisons may perform surveillance.	§ 126 2 (1), Chapter 3 of Criminal Procedure Law. https://www.riigiteataja.ee/akt/12749538?leiaKehtiv
Which LEAs can use this tool?	The Police and Border Guard Board, the Security Police Board, the Tax and Customs Board, the Military Police and the Prisons Department of the Ministry of Justice and prisons may perform surveillance.	§ 126 2 (1), Chapter 3 of Criminal Procedure Law. https://www.riigiteataja.ee/akt/12749538?leiaKehtiv
What are the rules to be followed for the implementation of this tool?	1) Surveillance acts shall not endanger the life and health of a person, unreasonably endanger property and the environment or unreasonably infringe other personal rights. 2) Surveillance acts shall be performed directly through the agencies specified in subsection 126 2 (1) of this Code as well as agencies administered by them and agencies, subdivisions and employees authorised to perform surveillance acts, as well as through police agents, undercover agents and persons involved in secret co-operation.	§ 126 1 (3 and 5), Chapter 3 of Criminal Procedure Law. https://www.riigiteataja.ee/akt/12749538?leiaKehtiv
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	The Prosecutor's Office shall issue a permit for covert surveillance of a person, thing or locality, covert collection of reference material and performance of preliminary investigations and covert examination or replacement of a thing for up to two months. The Prosecutor's Office may extend the term of the permit by up to two months.	§ 126-5 (1), Chapter 3 of Criminal Procedure Law. https://www.riigiteataja.ee/akt/12749538?leiaKehtiv
What ongoing supervision is required for the use of this tool?	No information found. But inference of the national law, there is no need of ongoing supervision is required, because everything is prepared before.	§ 126 2 (1), Chapter 3 of Criminal Procedure Law. https://www.riigiteataja.ee/akt/12749538?leiaKehtiv
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	

Source: Author's own elaboration

Finland

Table 26 – Overview of national rules on investigative tools - Finland

Relevant items	Provisions	Sources used
Controlled Delivery		
Relevant documents (legal and non-legal) that define the functioning of the tool	Coercive Measures Act (806/2011; entry into force on 1 January 2014) (amendments up to 1146/2013 included).	Translated version of the law: https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf
How is the tool defined?	"A criminal investigation authority may refrain from intervening in the transport or other delivery of an object, substance or property or transfer such intervention if this is necessary in order to identify persons participating in an offence that is being committed or in order to clarify an offence or larger offence entity that is more serious than the offence that is being committed".	Coercive Measures Act Chapter 10, Section 41 – Controlled delivery and its prerequisites: https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf

Relevant items	Provisions	Sources used
For what types of crime can the tool be used?	Cross crime areas (no limitations set)	Coercive Measures Act, Chapter 10: https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf
Does national law allow this tool to be used in cross-border cases?	The tool can be used in cross-border cases if this is agreed in international agreements binding on Finland or other obligations binding on Finland relating to international controlled delivery.	Coercive Measures Act Chapter 10, Section 41 – Controlled delivery and its prerequisites: https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf
What thresholds must be passed for the use of this tool?	"A criminal investigation authority may use controlled delivery if there are grounds to suspect an offence for which the most severe punishment provided is imprisonment for at least four years. A further prerequisite is that the delivery can be controlled and, if necessary, intervention in it can take place. In addition, the measure may not cause significant danger to the life, health or freedom of any person or the significant danger of extensive damage to the environment, to property or to assets".	Coercive Measures Act, Chapter 10, Section 41.2 https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf
What types of stakeholder are involved in the implementation of this tool?	Users of the tool: Police, Border Guard, Customs and military authorities Warrant providers/authorisation (Police and military authorities): The Chief of the National Bureau of Investigation, the Chief of the Security Intelligence Service or a police chief, or an official with the power of arrest, Warrant providers/authorisation (Customs): Head of Customs crime fighting unit or specifically assigned Customs employee responsible for undercover information gathering. Warrant providers/authorisation (Border guard): Head or Vice president of Border Guard's Justice department.	- Coercive Measures Act, Chapter 10, Section 42: https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf - Law regarding customs and crime fighting (in Finnish): https://www.finlex.fi/fi/laki/ajantasa/2015/20150623 - Law regarding Border Guard and crime fighting (in Finnish) https://www.finlex.fi/fi/laki/alkup/2018/20180108
Which LEAs can use this tool?	Police, Border Guard, Customs and military authorities.	Coercive Measures Act Chapter 10, Section 1.2: https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf
What are the rules to be followed for the implementation of this tool?	- A criminal investigation authority may refrain from intervening in the transport or other delivery of an object, substance or property or transfer such intervention if this is necessary in order to identify persons participating in an offence that is being committed or in order to clarify an offence or larger offence entity that is more serious than the offence that is being committed (controlled delivery). - A criminal investigation authority may use controlled delivery if there are grounds to suspect an offence for which the most severe punishment provided is imprisonment for at least four years. A further prerequisite is that the delivery can be controlled and, if necessary, intervention in it can take place. In addition, the measure may not cause significant danger to the life, health or freedom of any person or the significant danger of extensive damage to the environment, to property or to assets. - What is separately provided in law regarding international controlled delivery applies in addition to international agreements binding on Finland (such as the Naples II convention) or other obligations binding on Finland relating to international controlled delivery.	- Coercive Measures Act, Chapter 10, Section 41: https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf - Naples II convention https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3AI33051
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Such restrictions regarding controlled delivery are not mentioned in the law.	- Criminal code of Finland: https://www.finlex.fi/fi/laki/kaannokset/1889/en18890039.pdf - Coercive Measures Act: https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf
What authorisation is needed for the use of this tool?	1. Complete the warrant following the requirements on warrant (same for all of the LEAs): The warrant on controlled delivery shall specify: (1) the suspected offence and the time of its commission; (2) the person suspected in the offence; (3) the facts on the basis of which the person is suspected in the offence; (4) the goal of the collection of intelligence and the plan for its performance; (5) the transport or other delivery that is the object of the measure; (6) the validity of the warrant; (7) possible restrictions on and conditions for the controlled delivery. 2. Ask for authorization/Approval of warrant 2a) Authorization of warrant for police and military authorities: "The Chief of the National Bureau of Investigation, the Chief of the Security Intelligence Service or a police chief, or an official with the power of arrest especially trained in covert collection of intelligence and assigned with this function, decides on controlled delivery conducted by the police. Ask for authorisation/Approval of warrant 2a) Authorisation of warrant for police and military authorities: "The Chief of the National Bureau of Investigation, the Chief of the Security Intelligence Service or a police chief, or an official with the power of arrest especially trained in covert collection of intelligence and assigned with this function, decides on controlled delivery conducted by the police. Separate provisions apply to decision-making of other authorities on controlled delivery." 2b) Authorisation of Customs warrant: Head of Customs crime fighting unit or specifically assigned Customs employee responsible for undercover information gathering may authorize the warrant. 2c) Authorisation of Border Guard warrant: Head or Vice president of Border Guard's Justice department may authorize the warrant. 3. Follow the time limit (same for all of the LEAs): "The warrant for controlled delivery may be given for at most one month at a time."	- Coercive Measures Act, Chapter 10, Section 42: https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf - Law regarding customs and crime fighting (in Finnish): https://www.finlex.fi/fi/laki/ajantasa/2015/20150623 - Law regarding Border Guard and crime fighting (in Finnish) https://www.finlex.fi/fi/laki/alkup/2018/20180108

Relevant items	Provisions	Sources used
What ongoing supervision is required for the use of this tool?	- The National Police Board and the chiefs of units (Chief of National Bureau of Investigation, Chief of Finnish Security Intelligence Service or chiefs of Police departments). - The Ministry of the Interior shall submit an annual report to the Parliamentary Ombudsman on the use and supervision of covert coercive measures and their protection.(3) The Police Act contains provisions on reports to the Parliamentary Ombudsman on covert collection of intelligence for the prevention or detection of offences.	Coercive measures Act, Chapter 10, Section 65: https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf
Is there any national case law relating to the use of this tool in cross-border crime cases?	Case Law system is not used in Finland.	
Data available on the number of times this tool has been used for SOC cases	No exact statistics available. The police authorities of Finland reported in 2020 that controlled delivery was not used in 2019 and that the in total there have only few instances when the tool has been used.	Police authorities' report to Ministry of Interior on usage of investigative tools: https://intermin.fi/documents/1410869/4113506/Kertomus+poliisin+salaisten+pakkokeinojen+ja+tiedonhankintakeinojen+k%C3%A4yt%C3%B6st%C3%A4+2019/1b3a40a9-08fe-f649-66fa-53e4bccb45e5/Kertomus+poliisin+salaisten+pakkokeinojen+ja+tiedonhankintakeinojen+k%C3%A4yt%C3%B6st%C3%A4+2019.pdf
Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	Police Act (493/1995; amendments up to 560/2007 included).	https://www.finlex.fi/fi/laki/kaannokset/1995/en19950493_20070560.pdf
How is the tool defined?	"A competent government official of a State applying the Schengen acquis referred to in article 40 of the Convention implementing the Schengen Agreement on the gradual abolition of checks at the common borders (Schengen Convention) has the right to pursue and apprehend an offender caught in the act of committing an offence in the territory of the official's country or observed escaping from the territory of the official's country, in the territory of Finland and to carry out a security search on the offender in the territory of Finland, as provided in the Schengen acquis binding on Finland. The provisions of sections 21(1) and 22(1) and (5) also apply to the stopping of vehicles and security searches".	Police Act, Chapter 2, Section 22a.1: https://www.finlex.fi/fi/laki/kaannokset/1995/en19950493_20070560.pdf
For what types of crime can the tool be used?	Cross crime areas (no specific crime types mentioned).	Police Act, Chapter 2, Section 22a: https://www.finlex.fi/fi/laki/kaannokset/1995/en19950493_20070560.pdf
Does national law allow this tool to be used in cross-border cases?	Yes, it allows the usage of this tool in cross-border cases.	Police Act, Chapter 2, Section 22a.1: https://www.finlex.fi/fi/laki/kaannokset/1995/en19950493_20070560.pdf
What thresholds must be passed for the use of this tool?	No such thresholds are set in the Police Act. The right to use force in Hot Pursuit is limited: "the right to use force to apprehend a person caught in the act of committing an offence or who is in the process of escaping only applies to situations in which the person concerned offers resistance to avoid capture and competent Finnish officials are not immediately available for providing assistance in the apprehending".	Police Act, Chapter 2, Section 22a: https://www.finlex.fi/fi/laki/kaannokset/1995/en19950493_20070560.pdf
What types of stakeholder are involved in the implementation of this tool?	Users of the tool: Finnish Police or agreed Foreign Police Force in Finnish territory Authorisation: Depends on the specific agreement (e.g. The Schengen Convention, article 41. often applied).	Coercive Measures Act of Finland, Chapter 11, Section 3: https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf
Which LEAs can use this tool?	Only police authorities as Police Act concerns them.	Police Act: https://www.finlex.fi/fi/laki/kaannokset/1995/en19950493_20070560.pdf
What are the rules to be followed for the implementation of this tool?	Police Act, Chapter 2, Section 22a: Powers of government officials of foreign States (525/2005)(1) A competent government official of a State applying the Schengen acquis referred to in article 40 of the Convention implementing the Schengen Agreement on the gradual abolition of checks at the common borders (Schengen Convention) has the right to pursue and apprehend an offender caught in the act of committing an offence in the territory of the official's country or observed escaping from the territory of the official's country, in the territory of Finland and to carry out a security search on the offender in the territory of Finland, as provided in the Schengen acquis binding on Finland. The provisions of sections 21(1) and 22(1) and (5) also apply to the stopping of vehicles and security searches.(2) However, the right to use force to apprehend a person caught in the act of committing an offence or who is in the process of escaping only applies to situations in which the person concerned offers resistance to avoid capture and competent Finnish officials are not immediately available for providing assistance in the apprehending. What is provided elsewhere in this Act and in the Criminal Code (39/1889) also apply to the preconditions for and use of force.(3) A person apprehended under subsection 1 of this section shall, without delay, be handed over to the District Police of the municipality in which the apprehending took place, and the District Police shall also be notified of any other measures carried out in the territory of Finland and their consequences.(4) The provisions of section 47(2) on the paying of compensation apply to the compensation for damage caused to third parties by the action taken by the competent government official referred to in subsection 1.	Police Act, Chapter 2, Section 22a: https://www.finlex.fi/fi/laki/kaannokset/1995/en19950493_20070560.pdf
Safeguards provided by national criminal laws to protect the rights of the	Such restrictions regarding Hot Pursuit are not mentioned in the law.	Criminal code of Finland: https://www.finlex.fi/fi/laki/kaannokset/1889/en18890039.pdf

Relevant items	Provisions	Sources used
individuals, ensure proportionality, and protect rule of law (if any)		Coercive Measures Act: https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	It depends on the contract between countries if any authorisation is needed: "A criminal investigation authority receives from or gives to a criminal investigation authority of a foreign state in connection with the use of coercive measures and on the right of a criminal investigation authority of a foreign state to use the powers of a Finnish criminal investigation official related to coercive measures, what is separately provided or agreed thereon in an international agreement binding on Finland applies." Finland has a contract regarding police co-operation including hot pursuit with Norway and Sweden but as they are applying The Schengen Convention, article 41., the guidelines set by Schengen Convention are followed.	Coercive Measures Act of Finland, Chapter 11, Section 3: https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf
What ongoing supervision is required for the use of this tool?	The actual supervision is specified in individual contracts between countries but according to Police Act: "A person apprehended in Finland shall, without delay, be handed over to the District Police of the municipality in which the apprehending took place, and the District Police shall also be notified of any other measures carried out in the territory of Finland and their consequences."	Police Act, Chapter 2, Section 22a.3: https://www.finlex.fi/fi/laki/kaannokset/1995/en19950493_20070560.pdf
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	Law regarding witness protection program (6.2.2015/88).	Law regarding witness protection, only available in Finnish: https://finlex.fi/fi/laki/ajantasa/2015/20150088
How is the tool defined?	Witness protection program is a program that police in co-operation with other public officials carries out and in which person is protected from a serious illegal threat to person's life or health.	Law regarding witness protection, Section 1: https://finlex.fi/fi/laki/ajantasa/2015/20150088
For what types of crime can the tool be used?	Cross crime areas (no specific crime types mentioned).	Law regarding witness protection, only available in Finnish: https://finlex.fi/fi/laki/ajantasa/2015/20150088
Does national law allow this tool to be used in cross-border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	The individual to be protected 2) Police and other officials responsible for the protection 3) Head of National Bureau of Investigation making the decision on the program.	Law regarding witness protection, only available in Finnish: https://finlex.fi/fi/laki/ajantasa/2015/20150088
Which LEAs can use this tool?	The police (if the police request other public officials might be involved too).	Law regarding witness protection, only available in Finnish: https://finlex.fi/fi/laki/ajantasa/2015/20150088
What are the rules to be followed for the implementation of this tool?	The program may be started if there is a serious illegal threat to person's life or health and there is no other means to protect the individual 2) the protected individual must a) be aware of how the program works b) give a written consent for his/her participation c) report all aspects his obligations and personal circumstances d) be perceived to be suitable to participate 3) the program may be ended if the person protected asks for it, the apparent risk for health or life has vanished or due to negligence of person under protection.	Law regarding witness protection, Section 2 and 3 only available in Finnish: https://finlex.fi/fi/laki/ajantasa/2015/20150088
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Head of National Bureau of Investigation makes the decision on starting and ending of witness protection program, other authorisation is not needed.	Law regarding witness protection, Section 12: https://finlex.fi/fi/laki/ajantasa/2015/20150088
What ongoing supervision is required for the use of this tool?	National Police Board: supervises that Law regarding witness protection is followed 2) National Bureau of Investigation: Reports yearly to National Police Board on decisions made in relation to Law regarding witness protection 3) Ministry of Interior: Reports to the Parliamentary Ombudsman yearly regarding decisions made in relation to Law regarding witness protection	Law regarding witness protection, Section 14: https://finlex.fi/fi/laki/ajantasa/2015/20150088
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	In the first year when the tool was introduced National Bureau of Investigation told Finnish news that the tool was used 5-10 times.	Link to the piece of news: https://www.mtvuutiset.fi/artikkeli/krp-mtv-uutisille-suomessa-todistajansuojeluun-5-10-ihmista-ihmiselle-luodaan-uusi-elama/5703900

Relevant items	Provisions	Sources used
Surveillance		
Relevant documents (legal and non-legal) that define the functioning of the tool	Police act (493/1995; amendments up to 560/2007 included) and Coercive measures act ((806/2011; entry into force on 1 January 2014) (amendments up to 1146/2013 included)).	- Coercive measures Act: https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf - Police Act: https://www.finlex.fi/fi/laki/kaannokset/1995/en19950493_20070560.pdf
Specific range of application of the tool	Telecommunications interception, Traffic data monitoring, Obtaining location data, Obtaining base station data, Camera surveillance, On-site interception, Technical observation, Technical monitoring, Technical surveillance of a device.	Coercive Measures Act, Chapter 10, Sections 3, 6, 8, 10, 12, 16, 19, 21, 23: (https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf).
How is the tool defined?	Telecommunications interception: "Telecommunications interception refers to the monitoring, recording and other processing of a message sent to or transmitted from a network address or terminal end device through a public communications network". Traffic data monitoring: "Traffic data monitoring refers to the obtaining of identifying data regarding a message that has been sent from or received by a network address or terminal end device connected to a telecommunications network" Obtaining location data: "Data regarding a network address or terminal end device in his or her possession or that he or she otherwise is assumed to use" Obtaining base station data: "obtaining of information on the network address and terminal end devices of persons who have logged in or who are logging on to a telecommunications system through a certain base station." Camera surveillance: "using a camera or other corresponding technical device may be used in surveillance for visual observation or recording." On-site interception: "Listening, recording and other processing with a technical device, procedure or program" Technical monitoring: "the monitoring of movement of an object, substance or property with the use of a radio transmitter or other similar technical device or method or program separately placed therein or that is already therein." Technical observation: "refers to observation or recording, of the suspect in an offence or of premises or another place with a camera or similar technical device, procedure or program installed in such place" Technical surveillance of a device: "other than solely sensory surveillance, recording or other processing of the operation of a computer or other corresponding technical device or of the data or identification data contained therein, for the purpose of the investigation of a factor that is of significance for the clarification of an offence"	Coercive Measures Act, Chapter 10, Sections 3, 6, 8, 10, 12, 16, 19, 21, 23: (https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf).
For what types of crime can the tool be used?	Cross crime areas (no limitations set).	Coercive measures Act: https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf
Does national law allow this tool to be used in cross-border cases?	Yes, it allows the usage of this tool in cross-border cases.	Coercive measures Act: https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf
What thresholds must be passed for the use of this tool?	Police Act: 1) Police officers have the right to keep persons under surveillance in places other than a residence in order to prevent or intervene in the commission of an offence if the person's behaviour or other circumstances give cause to suspect that he or she would commit an offence. 2) For a purpose referred to in subsection 1, surveillance can also apply to persons outside domestic premises who may reasonably be suspected of contributing to an offence for which the maximum punishment provided is more severe than six months' imprisonment.	Police Act, Chapter 3, Section 30: https://www.finlex.fi/fi/laki/kaannokset/1995/en19950493_20070560.pdf
What types of stakeholder are involved in the implementation of this tool?	User of the tool: The Police. Authorisation/warrant issuer (other methods than Camera Surveillance): the Court system. Authorisation/decision (Camera Surveillance): an official with power to arrest.	Coercive Measures Act, Chapter 10, Sections 5, 9, 11, 13, 18, 21, 24: (https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf).
Which LEAs can use this tool?	Only the police may use this tool.	Coercive measures Act, Chapter 10, Section 1.2: https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf
What are the rules to be followed for the implementation of this tool?	Telecommunications interception: 1) the person under investigation is a suspect of serious crime 2) the user must have a warrant 3) the offence was committed in order to obtain especially large benefit and the offence has been committed in an especially methodical manner Traffic data monitoring: 1) the person under investigation is a suspect of serious crime 2) the user must have a warrant Obtaining location data: 1) the person under investigation is a suspect of serious crime 2) the user must have a warrant 3) there is reason to suspect that he or she is fleeing or otherwise evading the criminal investigation or court proceedings Obtaining base station data: 1) the person under investigation is a suspect of serious crime 2) the user must have a warrant. Camera surveillance: In longer term: 1) the person under investigation is a suspect of serious crime 2) the decision on using the tool must have been made by an official with power to arrest On-site interception: 1) A criminal investigation authority may direct on-site interception at a suspect in an offence outside of premises used as a permanent residence, and at a suspect in an offence who has been deprived of his or her liberty and is held in the premises of the authorities. The interception may be conducted by directing it at premises or at another place where the suspect can be presumed to be or visit 2) the person under investigation is a suspect of serious crime. 3) the user must have a warrant Technical observation: 1) the person under investigation is a suspect of serious crime 2) the user must have a warrant 3) Technical observation may not be directed at premises used as a permanent residence. Technical monitoring: 1) the person under investigation is a suspect of serious crime 2) the user must have a warrant Technical surveillance	Coercive Measures Act, Chapter 10, Sections 3, 6, 8, 10, 12, 16, 19, 21, 23: (https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf).

Relevant items	Provisions	Sources used
	of a device: 1) Technical surveillance of a device may not be used to obtain information about the content of a message or the identifying traffic data 2) The criminal investigation authority may direct technical surveillance of a device at a computer or another corresponding technical device or its program if the person under investigation is a suspect of serious crime 3) the user must have a warrant	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	Telecommunications interception: warrant from court Traffic data monitoring: warrant from court Obtaining location data: warrant from court, Obtaining base station data: warrant from court, Camera surveillance: An official's with the power of arrest decision On-site interception: warrant from court, Technical observation: warrant from court, Technical monitoring: warrant from court, Technical surveillance of a device: warrant from court. The request for a warrants shall specify: (1) the suspected offence and the time of its commission; (2) the person suspected in the offence; (3) the facts on the basis of which the person is suspected in the offence and which fulfil the prerequisites for the usage of tool; (4) the validity of the warrant, including the exact time; (5) the premises or other place that is the object of the tool usage; (6) the official with the power of arrest who is directing and supervising the performance of the tool usage; (7) possible restrictions on and conditions for the tool usage.	Coercive Measures Act, Chapter 10, Sections 5, 9, 11, 13, 18, 21, 24: (https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf).
Is there any national case law relating to the use of this tool in cross-border crime cases?	For all techniques mentioned above: (1) The National Police Board and the chiefs of units using covert coercive measures supervise the use of covert coercive measures on the part of the police. (2) The Ministry of the Interior shall submit an annual report to the Parliamentary Ombudsman on the use and supervision of covert coercive measures and their protection. (3) The Police Act contains provisions on reports to the Parliamentary Ombudsman on covert collection of intelligence for the prevention or detection of offences.	Coercive measures Act, Chapter 10, Section 65: (https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf)
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Undercover / covert operations		
Relevant documents (legal and non-legal) that define the functioning of the tool	Police act (493/1995; amendments up to 560/2007 included) and Coercive measures act ((806/2011; entry into force on 1 January 2014) (amendments up to 1146/2013 included)).	- Police Act: (https://www.finlex.fi/fi/laki/kaannokset/1995/en19950493_20070560.pdf) - Coercive measures act: (https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf)
How is the tool defined?	"Undercover activities means continuous or repeated gathering of information on individual persons or groups of persons or their activities with the help of infiltration".	Police Act, Chapter 3, Section 28.4.: (https://www.finlex.fi/fi/laki/kaannokset/1995/en19950493_20070560.pdf)
For what types of crime can the tool be used?	1) Criminals/suspected criminals who are breaking travel ban 2) Child pornography related crimes(e.g. production, sales, rental or distribution of child pornography)	- Police act, Chapter 3, Section 31a: (https://www.finlex.fi/fi/laki/kaannokset/1995/en19950493_20070560.pdf) - Coercive measures Act chapter 5a, section 2: (https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf) - Criminal code, Chapter 17, section 18(1)(1): (https://www.finlex.fi/fi/laki/kaannokset/1889/en18890039.pdf)
Does national law allow this tool to be used in cross-border cases?	Yes, it allows the usage of this tool in cross-border cases.	Police Act, Chapter 2, Section 22a.1: (https://www.finlex.fi/fi/laki/kaannokset/1995/en19950493_20070560.pdf)
What thresholds must be passed for the use of this tool?	- Police act Chapter 3, Section 31a: "Police officers have the right to undertake undercover activities if they are necessary to prevent, detect or investigate criminal activities referred to in Chapter 5a, section 2 of the Coercive Measures Act or an offence referred to in Chapter 17, section 18(1)(1) of the Criminal Code, or a punishable attempt of such an offence and the behaviour of the persons on whom information is gathered or other circumstances give reasonable cause to suspect that they could commit the offence in question. Undercover activities in places of residence are permitted if the entry or stay in the place of residence takes place with the active assistance of the occupant. However, provisions in the Coercive Measures Act apply to the search of premises." "Section 2 – Contents of a travel ban (1) The person subjected to a travel ban may be obliged to: (1) remain in the locality or area referred to in the decision; (2) remain away from or not move in an area referred to in the decision; (3) remain available at his or her residence or place of work at certain times; (4) present himself or herself to the police at certain times; (5) remain in an institution or hospital into which he or she has already	- Police act, Chapter 3, Section 31a: (https://www.finlex.fi/fi/laki/kaannokset/1995/en19950493_20070560.pdf) - Coercive measures Act chapter 5a, section 2: (https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf) - Criminal code, Chapter 17, section 18(1)(1): (https://www.finlex.fi/fi/laki/kaannokset/1889/en18890039.pdf)

Relevant items	Provisions	Sources used
	been admitted or is to be admitted; (6) refrain from contacting a person referred to in section 1, subsection 1, paragraph 2; or (7) surrender his or her passport to the police. (2) The decision on the travel ban may nonetheless include permission to leave said locality or area in order to go to work or for another comparable reason". A person who manufactures, offers for sale or for rent or otherwise offers or makes available, keeps available, exports, imports to or transports through Finland to another country, or otherwise distributes pictures or visual recordings that factually or realistically depict a child shall be sentenced for distribution of a sexually offensive picture to a fine or imprisonment for at most two years. (540/2011).	
What types of stakeholder are involved in the implementation of this tool?		
Which LEAs can use this tool?	Users of the tool: Police, Border Guard, Customs and military authorities. authorisation/decision maker: Head of a police unit that is laid down by Ministry of the Interior decree.	Police Act, Chapter 3, Section 32a: https://www.finlex.fi/fi/laki/kaannokset/1995/en19950493_20070560.pdf
What are the rules to be followed for the implementation of this tool?	Police mainly but Coercive measures act offer a possibility to Border Guard, Customs and military authorities to participate in covert activities too. All of them follow the same guidelines set by the Police Act	- Police Act Chapter 3, Section 28.4.: https://www.finlex.fi/fi/laki/kaannokset/1995/en19950493_20070560.pdf - Coercive measures Act, Chapter 10, Section 1: https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	There aren't further rules regarding this if crime type is as described in Police act Chapter 3, Section 31a and decision is made according to Section 32a Deciding on undercover activities and transactions and supervising undercover activities and transactions (525/2005): The decision on undercover activities shall be made by the head of a police unit that is laid down by Ministry of the Interior decree. (2) The decision on undercover transactions shall be made by a district police chief, the head of the National Bureau of Investigation or the head of the Security Police, or a commanding police officer to whom he or she has given responsibility for such decisions. (3) The police unit which has decided on undercover activities and transactions shall prepare a report on the activities for the Ministry of the Interior, which submits an annual report on the use of undercover activities and transactions to the Parliamentary Ombudsman.	Police Act, Chapter 3, Sections 32a and 31a: https://www.finlex.fi/fi/laki/kaannokset/1995/en19950493_20070560.pdf
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Such restrictions regarding Undercover/covert operations are not mentioned in the law.	- Criminal code of Finland: https://www.finlex.fi/fi/laki/kaannokset/1889/en18890039.pdf - Coercive Measures Act: https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf
What ongoing supervision is required for the use of this tool?	"Deciding on undercover activities and transactions and supervising undercover activities and transactions (525/2005) (1) The decision on undercover activities shall be made by the head of a police unit that is laid down by Ministry of the Interior decree. (2) The decision on undercover transactions shall be made by a district police chief, the head of the National Bureau of Investigation or the head of the Security Police, or a commanding police officer to whom he or she has given responsibility for such decisions. (3) The police unit which has decided on undercover activities and transactions shall prepare a report on the activities for the Ministry of the Interior, which submits an annual report on the use of undercover activities and transactions to the Parliamentary Ombudsman".	Police Act, Chapter 3, Section 32a: https://www.finlex.fi/fi/laki/kaannokset/1995/en19950493_20070560.pdf
Is there any national case law relating to the use of this tool in cross-border crime cases?	(1) The National Police Board and the chiefs of units using covert coercive measures supervise the use of covert coercive measures on the part of the police. (2) The Ministry of the Interior shall submit an annual report to the Parliamentary Ombudsman on the use and supervision of covert coercive measures and their protection. (3) The Police Act contains provisions on reports to the Parliamentary Ombudsman on covert collection of intelligence for the prevention or detection of offences.	Coercive measures Act, Chapter 10, Section 65: https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	Police act (493/1995; amendments up to 560/2007 included) and Coercive measures act ((806/2011; entry into force on 1 January 2014) (amendments up to 1146/2013 included)).	- Police Act: https://www.finlex.fi/fi/laki/kaannokset/1995/en19950493_20070560.pdf - Coercive measures act https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf
Specific range of application of the tool	Informant types not specified in Police Act or Coercive measures act.	- Police Act: https://www.finlex.fi/fi/laki/kaannokset/1995/en19950493_20070560.pdf - Coercive measures act https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf
How is the tool defined?	Use of human intelligence sources means the gathering of information using persons outside the police administration as information sources.	Police Act, Chapter 3, Section 28.8: https://www.finlex.fi/fi/laki/kaannokset/1995/en19950493_20070560.pdf
For what types of crime can the tool be used?	Cross crime areas (no limitations set).	Police Act: https://www.finlex.fi/fi/laki/kaannokset/1995/en19950493_20070560.pdf

Relevant items	Provisions	Sources used
Does national law allow this tool to be used in cross-border cases?	Yes, it allows the usage of this tool in cross-border cases.	Police Act, Chapter 2, Section 22a.1: https://www.finlex.fi/fi/laki/kaannokset/1995/en19950493_20070560.pdf
What thresholds must be passed for the use of this tool?	No limits set on this in Police Act or Coercive measures Act.	- Police Act: https://www.finlex.fi/fi/laki/kaannokset/1995/en19950493_20070560.pdf - Coercive measures act: https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf
What types of stakeholder are involved in the implementation of this tool?	Users of the tool: Police, Border Guard, Customs and military authorities. Authorisation/decision by one of the following: The Chief of the National Bureau of Investigation, the Chief of the Security Intelligence Service or a police chief, or an official with the power of arrest especially trained in covert collection of intelligence.	- Coercive Measures Act Chapter 10, Section 1.2: https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf - Coercive measures Act Chapter 10, Section 40: https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf
Which LEAs can use this tool?	Police, Border Guard, Customs and military authorities.	Coercive Measures Act Chapter 10, Section 1.2: https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf
What are the rules to be followed for the implementation of this tool?	The rules regarding the usage of informants are set in the following two laws: Police Act, Chapter 3, Section 36a: "Use of human intelligence sources (525/2005) (1) The police may, for carrying out its duties laid down in section 1, use persons outside the police administration as human intelligence sources. (2) The information on the human intelligence source may be entered in a personal data file. The provisions of the Act on the Processing of Personal Data by the Police (761/2003) apply to the processing of the information. (3) The person used as a human intelligence source may be paid a fee. The precondition for paying the fee is that the information source is registered. The fee may, on reasonable grounds, also be paid to a person used as a human intelligence source who has not been registered. Separate provisions shall be issued on the taxability of the fee." and Coercive measures Act Chapter 10, Section 39: "Use of covert human intelligence sources and prerequisites for the controlled use of covert human intelligence sources (1) The use of covert human intelligence sources refers to other than occasional reception by the police and other criminal investigation authorities of confidential information from a third party that is of significance in the clarification of an offence (human intelligence source). (2) The police may request for this purpose that an approved human intelligence source who has the suitable personal characteristics, is registered and who consents to the collection of intelligence, gather intelligence referred to in subsection 1 (controlled use of covert human intelligence sources). (3) In the controlled use of covert human intelligence sources, no request may be made for the collection of intelligence in a manner that would require the exercise of the powers of the authorities or that would endanger the life or health of the human intelligence source or another person. Before the controlled use of covert human intelligence sources, the human intelligence source shall be informed of his or her rights and obligations and in particular of what activity he or she may and may not do in accordance with law. As necessary the safety of the human intelligence source shall be ensured during and after the collection of the intelligence. (4) The Police Act contains provisions on the recording of data concerning a human intelligence source in a personal data file and on the payment of fees".	- Police Act, Chapter 3, Section 36a: https://www.finlex.fi/fi/laki/kaannokset/1995/en19950493_20070560.pdf - Coercive measures Act Chapter 10, Section 39: https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	(1) The authorisation must be received from one of the following persons: The Chief of the National Bureau of Investigation, the Chief of the Security Intelligence Service or a police chief, or an official with the power of arrest especially trained in covert collection of intelligence and assigned with this function, decides on the controlled use of covert human intelligence sources. (2) The decision on the controlled use of covert human intelligence sources may be given for at most six months at a time. (1146/2013) (3) The decision on the controlled use of covert human intelligence sources shall be made in writing. The decision shall specify: (1) who is requesting the measure; (2) the police unit that is conducting the collection of intelligence and the police officer who is responsible for its conduct; (3) the data identifying the source of intelligence; (4) the suspected offence; (5) the purpose and plan for conduct of the collection of intelligence; (6) the validity of the decision; (7) possible restrictions on and conditions for the controlled use of covert human intelligence sources. (4) The decision shall be reviewed as necessary in accordance with changes in circumstances. A written decision shall be made on the termination of the controlled use of covert human intelligence sources.	Coercive measures Act Chapter 10, Section 40: https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf
Is there any national case law relating to the use of this tool in cross-border crime cases?	(1) The National Police Board and the chiefs of units using covert coercive measures supervise the use of covert coercive measures on the part of the police. (2) The Ministry of the Interior shall submit an annual report to the Parliamentary Ombudsman on the use and supervision of covert coercive measures and their protection. (3) The Police Act contains provisions on reports	Coercive measures Act, Chapter 10, Section 65: https://www.finlex.fi/en/laki/kaannokset/2011/en20110806_20131146.pdf

Relevant items	Provisions	Sources used
	to the Parliamentary Ombudsman on covert collection of intelligence for the prevention or detection of offences.	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	N/A

Source: Author's own elaboration

France

Table 27 – Overview of national rules on investigative tools - France

Relevant items	Provisions	Sources used
Controlled Delivery		
Relevant documents (legal and non-legal) that define the functioning of the tool	Art. 706-80 to 706-80-2 of the Code of Criminal Procedure: Title XXV: On the procedure applicable to organised crime and delinquency and crimes. (De la procédure applicable à la criminalité et à la délinquance organisées et aux crimes).	Art. 706-80 to 706-80-2 of the Code of Criminal Procedure: Title XXV: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISC_TA000006138138/2021-02-25/
How is the tool defined?	The law does not provide a definition of "controlled delivery" but simply refers to it as: "[...]the supervision of the conveyance or transport of objects, goods or proceeds derived from or used in the commission of such offences.[...]" - by "such offences", it is meant the offences listed in articles 706-73, 706-73-1 and 706-74 of the Code of Criminal Procedure. Please refer to D10 for the list of offences.	Art. 706-80 Link: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000039279216
For what types of crime can the tool be used?	"Cross crime areas".	- Art. 706-73 Link: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000035937420 - Art. 706-73-1 Link: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000039183234 - Art. 706-74 Link: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000031052232
Does national law allow this tool to be used in cross-border cases?	The French code of criminal procedure does not provide any specific provisions when it comes to the cross-border implementation of controlled delivery. However, according to the questionnaire compiled by AMOC (Assessing resources against organised crimes) controlled delivery is a tool used in the context of cross-border investigations/operations.	Assessing Measures Against Organised Crime (AMOC). 2015. Study on paving the way for future policy initiatives in the field of fight against organised crime - effectiveness of specific criminal law measures targeting organised crime. Section 3. (Link unavailable)
What thresholds must be passed for the use of this tool?	The tool can be utilised only in the context of an investigation or enquiry into one of the crimes or offences failing within the scope of Article 706-73 and 706-73-1 of the Code of Criminal Procedure: Art. 706-73 1. Murder committed by an organised group (punished by life in prison) 2. Torture and acts of barbarity committed as an organised group (punishable by 30 years in prison); 3. Drug trafficking (punishable by life in prison) 4. Kidnapping committed as an organised group (punishable by life in prison) 5. Human trafficking (punishable by 15 years in prison) 6. Pimping (punishable by 10 years in prison) 7. Robbery committed as an organised group (punishable by 15 to 30 years in prison) 8. Extortion (punishable by 20 years in prison) 9. Felony of destroying, defacing or damaging property (punishable by 20 years in prison) 10. Counterfeit currency (punishable by 30 years in prison) 11. Acts of terrorism (punishable by life in prison) 11-bis. Crimes against the fundamental interests of the State 12. Misdemeanours relating to weapons and explosives (punishable by 10 years in prison) 13. Misdemeanours in relation to the illegal entry, movement and residence of a foreigner in France committed as an organised group (punishable by 5 years in prison) 14. Money Laundering (punishable by 5 years in prison) 15. Offences of criminal conspiracy when their object is the preparation of one of the offences mentioned in 1° to 14° and 17°. (punishable by 10 years in prison if the crime committed as a criminal association is punishable by 10 years in prison) 16. Offence of non-justification of resources corresponding to the lifestyle, when it is related to one of the offences mentioned in 1° to 15° and 17°. (punishable by 7 years in prison) 17. Crime of hijacking an aircraft, ship or any other means of transport committed by an organised group (punishable by 30 years in prison) 18. Crimes and offences punishable by 10 years' imprisonment, contributing to the proliferation of weapons of mass destruction and their means of delivery	- Art. 706-73 Link: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000035937420 - Art. 706-73-1 Link: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000039183234 - Art. 706-74 Link: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000031052232 - The penalties applicable to the crimes listed have been retrieved from the Penal Code: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000033975336/

Relevant items	Provisions	Sources used
	19. The offence of exploiting a mine or disposing of a substance subject to authorisation without a permit or authorisation, accompanied by environmental damage, committed as an organised group, when it is connected with one of the offences mentioned in 1° to 17° of this article. (punishable by 10 years in prison) Art. 706-73-1 1. The offence of fraud committed as an organised group, the offence of infringement of automated personal data processing systems implemented by the State committed as an organised group, and the offence of evasion committed as an organised group (punishable by 10 years in prison) 2. Offences of concealment of activities or employees, use of the services of a person carrying out concealed work, illegal labor trade or employment of foreigners without a work permit, committed as an organised group (punishable by 10 years in prison) 3. Offences of laundering or concealing the proceeds, income or things derived from the offences mentioned in 1. and 2. of this article (punishable by 5 years in prison) 3-bis. Money laundering offences with the exceptions of those mentioned in 14. of Article 706-73 (above) (punishable by 10 years in prison) 4. Criminal association whose purpose is to prepare one of the offences mentioned in 1. to 3. of this Article (punishable by 10 years in prison if the crime committed as a criminal association is punishable by 10 years in prison) 5. Non-justification of resources corresponding to the standard of living when it is related to one of the offences mentioned in 1. to 4. of the present article (punishable by 7 years in prison) 6. Import, export, transit, transport, possession, sale, acquisition or exchange of cultural property (punishable by 10 years in prison) 7. Offences against natural heritage committed by organised groups (punishable by 7 years in prison) 8. Offences of trafficking in plant protection products (produits phytopharmaceutiques) committed by organised groups (punishable by 5 years in prison) 9. Offences relating to waste committed as an organised group (punishable by 2 years in prison) 10. Offences of participation in the management of a gambling house committed as an organised group and offences of importing, manufacturing, holding, making available to third parties, installing and operating gambling machines as an organised group (punishable by 7 years in prison) 11. Offences affecting the fundamental interests of the State (punishable by 10 years in prison) Art. 706-74 1. Crimes and offences committed as an organised group, other than those falling under Articles 706-73 and 706-73-1 2. Offences of criminal association other than those falling under 15° of Article 706-73 or 4° of Article 706-73-1 of this Code.	
What types of stakeholder are involved in the implementation of this tool?	The following actors are involved in the context of Controlled Deliveries: -District prosecutor (<i>procureur de la République</i>) in charge of the investigation: The district prosecutor can grant approval (or not) of the performance of a controlled delivery (to be applied on the whole national territory) by the judicial police. Additionally, the district prosecutor is responsible for. 1. authorizing the judicial police to request any civil servant or public official to not carry out controls/seizures of objects, property or products subject to controlled delivery in order to not jeopardize the investigation. 2. eventually provide an authorisation ensuring that the judicial police to not be held criminally liable when delivering the objects, goods or products subject to controlled delivery at the place of delivery providers and freight operators. -District prosecutor (<i>procureur de la République</i>) of the jurisdiction in which the controlled delivery is likely to take place: The district prosecutor of the jurisdiction in which the controlled delivery is likely to take place is also responsible for granting approval and must be informed by the judicial police before initiating the controlled delivery. -District prosecutor (<i>procureur de la République</i>) of the Paris Court: - The district prosecutor of the Paris Court must be informed of any authorisations granted by the district prosecutor in charge of the investigation requesting civil servants/public officials to not carry out controls/seizures of objects, property or products subject to controlled delivery. -Investigating judge (<i>juge d'instruction</i>) Only after having notified (in advance) the district prosecutor in charge of the investigation, the investigating judge can: 1. authorize the judicial police to request civil servants or public officials to not carry out controls/seizures of objects, property or products subject to controlled delivery.	The actors involved in undercover operations are detailed from Article 706-80 to Art. 706-80-2 of the Code of Criminal Procedure Link: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISC_TA000006138138/2021-02-25/

Relevant items	Provisions	Sources used
	2. provide an authorisation ensuring that the judicial police to not be held criminally liable when delivering the objects, goods or products subject to controlled delivery at the place of delivery providers and freight operators. -Judicial Police Officer and Agents (<i>officier et agents de police judiciaire</i>) Judicial police officers and, under their authority, judicial police agents are responsible for carrying out controlled delivery (upon receiving the needed authorisations. In the context of a controlled delivery, judicial police officers are responsible for: -requesting civil servants or public officials to not carry out controls/seizures of objects, property or products subject to controlled delivery. -eventually deliver objects, goods or products subject to controlled delivery at the place of delivery provided and freight operators.	
Which LEAs can use this tool?	Judicial Police; Customs.	- Customs: Article 67 bis: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000041783841 - Judicial Police: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISC_TA000006138138/2021-02-25/
What are the rules to be followed for the implementation of this tool?	The following rules must be followed when implementing this tool: - Controlled delivery can be conducted by the judicial police only after having informed the district prosecutor (who has to grant approval) and the district prosecutor of the jurisdiction where controlled delivery will take place. [Art. 706-80] - There must be plausible reasons to suspect that the objects, goods or products subject to controlled delivery are derived from the commission of the offences listed in D10. [Art. 706-80] - Civil servants and public officials can be asked to not control or seizure objects, property or products subject to controlled delivery only after having obtained authorization by the district prosecutor in charge of the investigation (or the investigative judge, after having informed the district prosecutor). Civil servants and public officials can be asked to not control or seizure objects, property or products subject to controlled delivery only after having obtained authorisation by the district prosecutor in charge of the investigation (or the investigative judge, after having informed the district prosecutor). [Art. 706-80-1] - The authorisation of the district prosecutor or the investigating judge, which may be given by any means, shall be mentioned or included in the record of the proceedings. The District Prosecutor shall immediately inform the District Prosecutor at the Paris Court of the issuance of such authorisation. [Art. 706-80-1] - Under the authorisation of the district prosecutor in charge of the investigation (or the investigating judge), the judicial police is not held criminally liable for delivering objects, property or products subject to controlled delivery. [Art. 706-80-2] - Under penalty of nullity, the authorisation of the district prosecutor or investigating judge must be in writing and must state the reasons for the authorisation. This authorisation shall be entered in the record of the proceedings and the authorised acts may not constitute incitement to commit an offence.[Art. 706-80-2]	The rules relating to the conduction of undercover operations are detailed from Article 706-810to Art. 706-80-2 of the Code of Criminal Procedure. Please refer to the specific references inserted into the text (e.g. [Art. 706-80-1]) to identify the information provided in the text of the law. Link: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISC_TA000006138138/2021-02-25/
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	- There must be plausible reasons to suspect that the objects, goods or products subject to controlled delivery are derived from the commission of the offences listed in D10. [Art. 706-80] - Under penalty of nullity, the authorisation of the district prosecutor or investigating judge must be in writing and must state the reasons for the authorisation. This authorisation shall be entered in the record of the proceedings and the authorised acts may not constitute incitement to commit an offence.[Art. 706-80-2]	The rules relating to the conduction of undercover operations are detailed from Article 706-810to Art. 706-80-2 of the Code of Criminal Procedure. Please refer to the specific references inserted into the text (e.g. [Art. 706-80-1]) to identify the information provided in the text of the law. Link: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISC_TA000006138138/2021-02-25/
What authorisation is needed for the use of this tool?	- Controlled delivery can be conducted by the judicial police only after having informed the district prosecutor (who has to grant approval) and the district prosecutor of the jurisdiction where controlled delivery will take place. [Art. 706-80] - Civil servants and public officials can be asked to not control or seizure objects, property or products subject to controlled delivery only after having obtained authorization by the district prosecutor in charge of the investigation (or the investigative judge, after having informed the district prosecutor). Civil servants and public officials can be asked to not control or seizure objects, property or products subject to controlled delivery only after having obtained authorisation by the district prosecutor in charge of the investigation (or the investigative judge, after having informed the district prosecutor). This authorisation can be granted by any means and shall be included in the record of the proceedings. The District Prosecutor shall immediately inform the District Prosecutor at the Paris Court of the issuance of this authorisation. [Art. 706-80-1] - The judicial police is not held liable for delivering objects, property or products subject to controlled delivery only after having obtained authorisation from the district prosecutor in charge of the investigation (or the investigative judge, after having informed the	The rules regulating the authorisations of activities related to controlled delivery are detailed from Article 706-80 to Art. 706-80-2 of the Code of Criminal Procedure. Link: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISC_TA000006138138/2021-02-25/

Relevant items	Provisions	Sources used
	district prosecutor). Under penalty of nullity, this authorisation must be in writing and must state the reasons for the authorisation. This authorisation shall be entered in the record of the proceedings and the authorised acts may not constitute incitement to commit an offence. [Art. 706-80-2]	
What ongoing supervision is required for the use of this tool?	- When implementing the investigative tool, the judicial police officer is responsible for supervising any activities conducted by the judicial police agent. The district prosecutors in charge of the investigation is responsible for supervision the implementation of this investigative tool. - When it comes specifically to requesting civil servants or public officials to not carry out controls and seizure of objects, property or products subject to controlled delivery, the district prosecutor of the Paris court must be informed by the district prosecutor in charge of the investigation.	The rules regulating the authorisations of activities related to controlled delivery are detailed from Article 706-80 to Art. 706-80-2 of the Code of Criminal Procedure. Link: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISC_TA000006138138/2021-02-25/
Is there any national case law relating to the use of this tool in cross-border crime cases?	Cour de cassation – Criminal chamber - 23 mai 2017 / n° 16-87.323 Facts of the case: French authorities were alerted to the arrival of a vehicle from Marseille to department of Seine-Saint-Denis with the aim to load a high quantity of cocaine. Judicial police officers informed the district prosecutor of the Bobigny jurisdiction, as the article 706-80 requires to notify the district prosecutor of the place where the controlled delivery is likely to take place. The defendant asked for the annulment of the procedure as the controlled delivery took place in another district as the vehicle changed the planned itinerary. Therefore, the authorities informed the wrong district prosecutor Decision: The French supreme court upheld the judgment handed down on appeal refusing the nullity of the controlled delivery. The court stated that this kind of operation is subject to uncertainties and there is a need to act quickly. As a result, the law does not require that the public prosecutor's office with territorial jurisdiction to be informed has to be the one where the surveillance operations will be carried-out with certainty but the one where the controlled delivery is likely to start, within the limits of the information available at the time the public prosecutor is informed. This case gave practical precisions concerning the terms and conditions to implement the controlled delivery.	Link to the decision: https://www.legifrance.gouv.fr/juri/id/JURITEXT000034813392?init=true&page=1&query=23+mai+2017+%2F+n%C2%B0+16-87.323&searchField=ALL&tab_selection=all
Data available on the number of times this tool has been used for SOC cases	N/A	
Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	When it comes to hot pursuit, the following statutes are applicable: - Article 41 of the Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders Agreement signed with the Netherlands: - Décret n° 2015-1270 du 13 octobre 2015 portant publication de l'accord entre le Gouvernement de la République française et le Gouvernement du Royaume des Pays-Bas relatif à la coopération insulaire en matière policière à Saint-Martin (ensemble deux annexes), signé à Paris le 7 octobre 2010 Agreement signed with Germany: Décret n° 2000-924 du 18 septembre 2000 portant publication de l'accord entre le Gouvernement de la République française et le Gouvernement de la République fédérale d'Allemagne relatif à la coopération dans leurs zones frontalières entre les autorités de police et les autorités douanières (ensemble une déclaration), signé à Mondorf-les-Bains le 9 octobre 1997 Agreement signed with Switzerland: - Article 13 du Décret n° 2009-836 du 7 juillet 2009 portant publication de l'accord entre le Gouvernement de la République française et le Conseil fédéral suisse relatif à la coopération transfrontalière en matière judiciaire, policière et douanière, signé à Paris le 9 octobre 2007 Agreement signed with Belgium: - Décret n° 2015-1297 du 15 octobre 2015 portant publication de l'accord entre le Gouvernement de la République française et le Gouvernement du Royaume de Belgique relatif à la coopération transfrontalière en matière policière et douanière, signé à Tournai le 18 mars 2013 Agreement signed with Luxembourg: - Décret n° 2016-1294 du 29 septembre 2016 portant publication de l'accord entre le Gouvernement de la République française et le Gouvernement du Grand-Duché de Luxembourg relatif à la coopération dans leurs zones frontalières entre les autorités de police et les autorités douanières, signé à Luxembourg, le 15 octobre 2001 Agreement signed with Spain	- Agreement with Italy https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000766303?isSuggest=true - Agreement with Switzerland: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000020830546?init=true&isAdvancedResult=true&page=1&pageSize=10&query=%7B%28%40ALL%5Bt%22poursuite+transfrontali%C3%A8re%22%5D%29%7D&tab_selection=all&typeRecherche=date - Agreement with Spain: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000796362?init=true&page=1&query=coop%C3%A9ration+transfrontali%C3%A8re+en+mati%C3%A8re+polici%C3%A8re+et+douani%C3%A8re&searchField=ALL&tab_selection=all - Agreement with the Netherlands: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000031313014?init=true&isAdvancedResult=true&page=1&pageSize=10&query=%7B%28%40ALL%5Bt%22poursuite+transfrontali%C3%A8re%22%5D%29%7D&tab_selection=all&typeRecherche=date - Agreement with Belgium: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000031328288?init=true&isAdvancedResult=true&page=1&pageSize=10&query=%7B%28%40ALL%5Bt%22poursuite+transfrontali%C3%A8re%22%5D%29%7D&tab_selection=all&typeRecherche=date - Agreement with Germany: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000585254?isSuggest=true - Agreement with Luxembourg: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033172518?isSuggest=true - Agreement between Luxembourg, Germany, France and Belgium https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033172518?isSuggest=true

Relevant items	Provisions	Sources used
	-Décret n° 2003-915 du 19 septembre 2003 portant publication du traité entre la République française et le Royaume d'Espagne relatif à la coopération transfrontalière en matière policière et douanière, signé à Blois le 7 juillet 1998 Agreement signed with Italy: -Décret n°o 2000-923 du 18 septembre 2000 portant publication de l'accord entre le Gouvernement de la République française et le Gouvernement de la République italienne relatif à la coopération transfrontalière en matière policière et douanière, signé à Chambéry le 3 octobre 1997 Agreement between Luxembourg, France, Belgium and Germany: Accord entre le Gouvernement de la République française, le Gouvernement du Royaume de Belgique, le Gouvernement de la République fédérale d'Allemagne et le Gouvernement du Grand-Duché de Luxembourg concernant la mise en place et l'exploitation d'un centre commun de coopération policière et douanière dans la zone frontalière commune, signé à Luxembourg le 24 octobre 2008	
How is the tool defined?	Article 41 of the Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders defines hot pursuit as follows: "Officers of one of the Contracting Parties who are pursuing in their country an individual caught in the act of committing or of participating in one of the offences referred to in [D22] [...]"	Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:42000A0922(02)&from=EN
For what types of crime can the tool be used?	Hot pursuit is authorised for the following criminal offences (Paragraph 4 of article 41): Drugs; Illicit tobacco trade; Financial Crime (forgery of money); Trafficking of firearms; Illegal immigration	Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:42000A0922(02)&from=EN
Does national law allow this tool to be used in cross-border cases?	Hot pursuit is per se a cross-border investigation tool.	
What thresholds must be passed for the use of this tool?	Hot pursuit is authorised for the following criminal offences (Paragraph 4 of article 41): Drugs; Illicit tobacco trade; Financial Crime (forgery of money); Trafficking of firearms; Illegal immigration	Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:42000A0922(02)&from=EN
What types of stakeholder are involved in the implementation of this tool?	The following actors are involved in the implementation of the tool(Paragraph 7, Article 41): -criminal police officers of the national police and national 'gendarmerie' -customs officers Between Switzerland and France: As soon as the border is crossed, the hot pursuit must be communicated to the joint centres established between the two countries, which will inform the authorities: - for the French Republic: the district prosecutor of the jurisdiction where the hot pursuit takes place; - for Switzerland: the cantonal police commander and the commander of the competent customs agents. The agents who can engage in an hot pursuit are: - for the French Republic: officers and agents of the judicial police of the national police and the national gendarmerie, as well as customs officers, with regard to their powers relating to the illicit trafficking of narcotic drugs and psychotropic substances, trafficking in arms and explosives and the illicit transport of toxic or harmful materials and waste; - for Switzerland: officers of the federal and cantonal police forces and of the border guard corps. Between the Netherlands and France: The pursuit must be notified, at the latest when the border is crossed: - for the French Party: to the operational centre of the Saint-Martin gendarmerie, which will notify the district prosecutor with territorial jurisdiction; - for the Dutch Party: at the central police station of Sint-Maarten, Sint Eustatius and Saba, which shall notify the Attorney General of the Netherlands (Antilles). The pursuing officers shall be : - for the French Party: officers, judicial police officers and deputy judicial police officers of the national police and the national gendarmerie; - for the Netherlands Party: judicial police officers within the meaning of the Code of Criminal Procedure of the Netherlands Antilles. Between Germany and France: The cross-border hot pursuit must be communicated at the latest at the time of crossing the border :	- Agreement with Italy https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000766303?isSuggest=true - Agreement with Switzerland: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000020830546?init=true&isAdvancedResult=true&page=1&pageSize=10&query=%7B%28%40ALL%5Bt%22poursuite+transfrontali%C3%A8re%22%5D%29%7D&tab_selection=all&typeRecherche=date - Agreement with Spain: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000796362?init=true&page=1&query=coop%C3%A9ration+transfrontali%C3%A8re+en+mati%C3%A8re+polici%C3%A8re+et+douani%C3%A8re&searchField=ALL&tab_selection=all - Agreement with the Netherlands: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000031313014?init=true&isAdvancedResult=true&page=1&pageSize=10&query=%7B%28%40ALL%5Bt%22poursuite+transfrontali%C3%A8re%22%5D%29%7D&tab_selection=all&typeRecherche=date - Agreement with Belgium: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000031328288?init=true&isAdvancedResult=true&page=1&pageSize=10&query=%7B%28%40ALL%5Bt%22poursuite+transfrontali%C3%A8re%22%5D%29%7D&tab_selection=all&typeRecherche=date - Agreement with Germany: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000585254?isSuggest=true - Agreement with Luxembourg: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033172518?isSuggest=true - Agreement between Luxembourg, Germany, France and Belgium: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033172518?isSuggest=true

Relevant items	Provisions	Sources used
	-In the French Republic, to the joint centres established between the two countries, which will notify the district prosecutor of the jurisdiction in which the hot pursuit takes place. -In the Federal Republic of Germany: a) In Baden-Württemberg, to the Landespolizeidirektion in Freiburg or the Landespolizeidirektion in Karlsruhe; b) in Rhineland-Palatinate, at the police presidencies (Polizeipräsidium) in Rheinpfalz or Westpfalz; c) in Saarland, at the regional criminal police office (Landeskriminalamt). Between Italy and France: French Republic: the national police, the national gendarmerie, the customs. Italian Republic: state police, Carabinieri, Finance guard, Customs. Between Spain and France: French Republic: the national police, the national gendarmerie, the customs. Spain: National Police Corps, Civil Guard, all other services or police authorities chosen by the Ministry of the Interior. Between Luxembourg and France: French Republic (in the two border departments of Moselle and Meurthe-et-Moselle): the national police, the national gendarmerie, the customs. Luxembourg: the grand-ducal police, the customs. Between Luxembourg, France, Germany and Belgium (common agreement): A common centre between the four countries is established to ensure that the following authorities can collaborate in operations (such as hot pursuits): On the French side : the national police; the national gendarmerie; the customs and excise administration. On the Belgian side: the federal police; the local police; the customs and excise administration. On the German side : the police forces of the Länder of Rhineland-Palatinate and Saarland, the federal police, the customs administration; if necessary, the Federal Criminal Police Office. On the Luxembourg side : the grand-ducal police; the customs and excise administration.	
Which LEAs can use this tool?	The following LEAs are involved in the implementation of the tool(Paragraph 7, Article 41): -criminal police officers of the national police and national 'gendarmerie' -customs officers	• Agreement with Italy https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000766303?isSuggest=true • Agreement with Switzerland: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000020830546?init=true&isAdvancedResult=true&page=1&pageSize=10&query=%7B%28%40ALL%5Bt%22poursuite+transfrontali%C3%A8re%22%5D%29%7D&tab_selection=all&typeRecherche=date • Agreement with Spain: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000796362?init=true&page=1&query=coop%C3%A9ration+transfrontali%C3%A8re+en+mati%C3%A8re+polici%C3%A8re+et+douani%C3%A8re&searchField=ALL&tab_selection=all • Agreement with the Netherlands: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000031313014?init=true&isAdvancedResult=true&page=1&pageSize=10&query=%7B%28%40ALL%5Bt%22poursuite+transfrontali%C3%A8re%22%5D%29%7D&tab_selection=all&typeRecherche=date • Agreement with Belgium: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000031328288?init=true&isAdvancedResult=true&page=1&pageSize=10&query=%7B%28%40ALL%5Bt%22poursuite+transfrontali%C3%A8re%22%5D%29%7D&tab_selection=all&typeRecherche=date • Agreement with Germany: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000585254?isSuggest=true • Agreement with Luxembourg: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033172518?isSuggest=true • Agreement between Luxembourg, Germany, France and Belgium: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033172518?isSuggest=true
What are the rules to be followed for the implementation of this tool?	The following rules must be followed when implementing the tool (Article 41 of the Schengen Agreement): • Officer of one of the Contracting Parties who are pursuing in their country an individual caught in the act of committing or participating in one of the offences referred to in [D22] shall be authorised to continue pursuit in the territory of another Contracting Party without the latter's prior authorisation where, given the particular urgency of the situation, it is not possible to notify the competent authorities of the other Contracting Party or where these authorities are unable to reach the scene in time to take over the pursuit.	• Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:42000A0922(02)&from=EN • Agreement with Italy https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000766303?isSuggest=true • Agreement with Switzerland: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000020830546?init=true&isAdvancedResult=true&page=1&pageSize=10&query=%7B%28%40ALL%5Bt%22poursui

Relevant items	Provisions	Sources used
	- The pursuing officers shall contact the competent authorities of the Contracting Party in whose territory the hot pursuit is to take place no later than when they cross the border. The hot pursuit ceases as soon as the Contracting Party in whose territory the pursuit is taking place so requests. At the request of the pursuing officers, the competent local authorities shall challenge the pursued person in order to establish the person's identity or to make an arrest. - The pursuing officers shall not have the right to apprehend the pursued person. If no request to cease the hot pursuit is made and if the competent local authorities are unable to intervene quickly enough, the pursuing officers may detain the person pursued until the officers of the Contracting Party in whose territory the pursuit is taking place, who must be informed immediately, are able to establish the person's identity or make an arrest. - The pursuing officers must comply with the law of the Contracting Party in whose territory they are operating. - Pursuit shall be solely over land borders. - Entry into private homes and places not accessible to the public shall be prohibited. - The pursuing officers shall be easily identifiable, either by their uniform, by means of an armband or by accessories fitted to their vehicles. The use of civilian clothes combined with the use of unmarked vehicles without the aforementioned identification is prohibited. The pursuing officers must at all times be able to prove that they are acting in an official capacity. - The pursuing offices may carry their service weapons. Use of the weapons shall be prohibited save in cases of legitimate self-defence. - A person that has been apprehended in the context of a hot pursuit can only be subject to a security search: handcuffs may be used during the transfer, objects carried by the pursued person may be seized. - After the hot pursuit, the pursuing officers shall appear before the competent local authorities of the Contracting Party in whose territory they were operating and shall report on their mission. They shall remain at the disposal of the local authorities until the circumstances surrounding their action have been sufficiently clarified. This applies also in the event of hot pursuit not resulting with an arrest. - The authorities of the Contracting Party from which the pursuing officer have come shall assist the enquiry subsequent to the operation in which they took part, including judicial proceedings. - If the person arrested following an hot pursuit is not a national of the Contracting Party in whose territory the person was arrested, that person shall be released no later than six hours after the arrest was made, not including the hours between midnight and 9:00 AM, unless the competent local authorities have previously received request for that person's provisional arrest for the purposes of extradition in any form whatsoever. - The Contracting Party in which the pursuing officers operate shall be held liable for any damage caused by them during the hot pursuit in accordance with the law of the Contract Party in whose territory the hot pursuit took place. Specific rules for hot pursuit between Switzerland and France: - At the latest when crossing the border, the pursuing officers shall call upon the competent services of the Party in whose territory the pursuit takes place. The pursuit shall be stopped as soon as the Party in whose territory the pursuit is to take place so requests. At the request of the pursuing officers, the locally competent services shall apprehend the person pursued in order to establish his or her identity or arrest him or her. - The pursuing officers shall not have the right of arrest. - The pursuit must be communicated, at the latest when the border is crossed, to the joint centres, which shall inform the authorities of the pursuit: - for the French Republic: the district prosecutor with territorial jurisdiction; - for Switzerland: the cantonal police commander and the commander of the competent custom agents. - The joint centres inform the national central services of cross-border prosecutions carried out - Prosecution may be carried out without any limitation in space or time. - The officers responsible for prosecution are : - for the French Republic: officers and agents of the judicial police of the national police and the national gendarmerie, as well as customs officers, with regard to their powers relating to the illicit trafficking of narcotic drugs and psychotropic substances, trafficking in arms and explosives and the illicit transport of toxic or harmful materials and waste; - for Switzerland: officers of the federal and cantonal police forces and of the customs. - Hot pursuit can only take place under the following general conditions:	te+transfrontali%C3%A8re%22%5D%29%7D&tab_selection=all&typeRecherche=date - Agreement with Spain: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000796362?init=true&page=1&query=coop%C3%A9ration+transfrontali%C3%A8re+en+mati%C3%A8re+polici%C3%A8re+et+douani%C3%A8re&searchField=ALL&tab_selection=all - Agreement with the Netherlands: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000031313014?init=true&isAdvancedResult=true&page=1&pageSize=10&query=%7B%28%40ALL%5Bt%22poursuite+transfrontali%C3%A8re%22%5D%29%7D&tab_selection=all&typeRecherche=date - Agreement with Belgium: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000031328288?init=true&isAdvancedResult=true&page=1&pageSize=10&query=%7B%28%40ALL%5Bt%22poursuite+transfrontali%C3%A8re%22%5D%29%7D&tab_selection=all&typeRecherche=date - Agreement with Germany: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000585254?isSuggest=true - Agreement with Luxembourg: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033172518?isSuggest=true - Agreement between Luxembourg, Germany, France and Belgium: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033172518?isSuggest=true

Relevant items	Provisions	Sources used
	(a) The pursuing officers shall be easily identifiable, either by the wearing of a uniform, an armband or accessory devices placed on the vehicle; the use of civilian clothing combined with the use of unmarked vehicles without the above-mentioned identification is prohibited; (b) At the end of each pursuit, the pursuing officers shall immediately report to the locally competent services of the Party in whose territory they have operated and shall give an account of their mission; at the request of those services, they shall be obliged to remain at their disposal until the circumstances of their action have been sufficiently clarified; this condition shall apply even where the pursuit has not led to the arrest of the person pursued; (c) The use of air and waterborne means shall be permitted, in accordance with the law of each Party, and a technical arrangement shall specify the modalities. 8) A person who, at the end of the pursuit, has been arrested by the locally competent services may, whatever his or her nationality, be detained for questioning, within the limits of the law of the Party in whose territory the arrest took place. If that person does not have the nationality of the Party in whose territory he or she was arrested, he or she shall be released not later than six hours after the arrest, not counting the hours between midnight and nine o'clock, unless the locally competent authorities have received, before the expiry of that period, a notice announcing a request for provisional arrest for the purpose of extradition in any form whatsoever. Specific rules for hot pursuit between Netherlands and France: 1) At the latest when crossing the border, the pursuing officers shall call upon the competent services of the Party in whose territory the pursuit takes place. The pursuit shall be stopped as soon as the Party in whose territory the pursuit is to take place so requests. At the request of the pursuing officers, the locally competent services shall apprehend the person pursued in order to establish his or her identity or arrest him or her. 2) The pursuing officers shall not have the right of arrest. 3) The pursuit must be notified, at the latest when the border is crossed: - for the French Party: to the operational centre of the Saint-Martin gendarmerie, which will notify the district prosecutor with territorial jurisdiction; - for the Dutch Party: at the central police station of Sint-Maarten, Sint Eustatius and Saba, which shall notify the Attorney General of the Netherlands (Antilles). 4) Hot pursuit may be instituted without limitation as to space and time. 5) The pursuing officers shall be: - for the French Party: officers, judicial police officers and deputy judicial police officers of the national police and the national gendarmerie; - for the Netherlands Party: judicial police officers within the meaning of the Code of Criminal Procedure of the Netherlands Antilles. 6) Prosecution may only take place under the following general conditions: (a) The pursuing officers shall be readily identifiable either by the wearing of a uniform or an armband or by means of accessory devices placed on the vehicle; the use of civilian clothing combined with the use of unmarked vehicles without the specified identification shall be prohibited. (b) At the end of each pursuit, the pursuing officers shall immediately report to the locally competent services of the Party in whose territory they have been operating and shall give an account of their mission; at the request of those services, they shall be obliged to remain at their disposal until the circumstances of their action have been sufficiently clarified; this condition shall apply even where the pursuit has not led to the arrest of the person pursued; (c) The use of air and waterborne means shall be permitted in accordance with the law of each Party; a technical arrangement shall specify the modalities. 7) A person who, at the end of the hot pursuit, has been arrested by the locally competent authorities may, whatever his or her nationality, be detained for questioning, within the limits of the law of the Party in whose territory the arrest took place. If that person does not have the nationality of the Party in whose territory he or she was arrested, he or she shall be released not later than six hours after his or her arrest, not counting the hours between midnight and 9 a.m., unless the locally competent authorities have received, before the expiry of that period, a notice announcing a request for provisional arrest for the purpose of extradition in any form whatsoever. Specific rules for hot pursuit between Germany and France: 1) Cross-border hot pursuit is carried out in accordance with Article 41 of the Convention Implementing the Schengen Agreement. It is possible to enter workplaces, company or business premises accessible to the public during their respective opening hours. 2) The cross-border hot pursuit must be communicated at the latest at the time of crossing the border: - In the French Republic, to the joint centres established between the two countries, which will notify the district prosecutor of the jurisdiction in which the hot pursuit takes place. - In the Federal Republic of Germany: a) In Baden-Württemberg, to the Landespolizeidirektion in Freiburg or the Landespolizeidirektion in Karlsruhe;	

Relevant items	Provisions	Sources used
	b) in Rhineland-Palatinate, at the police presidencies (Polizeipräsidentium) in Rheinpfalz or Westpfalz; c) in Saarland, at the regional criminal police office (Landeskriminalamt). Changes concerning these competences are notified to the other Contracting Party. 3) The locally competent authority (in the French Republic, the district prosecutor of the jurisdiction in which the hot pursuit takes place) may request the discontinuation of proceedings. 4) In cases of particular seriousness or where the prosecution has gone beyond the border area, the national central authorities should be informed. 5) In the event of a cross-border observation or pursuit, police or customs officers of the neighbouring State shall be subject to the same legal provisions as regards traffic as the police and customs officers of the Contracting Party in whose territory the observation or pursuit is carried out. The Contracting Parties shall inform each other of the regulations in force on this point. 6) The technical means necessary to facilitate trans frontier observation or pursuit may be used in so far as this is permitted by the law of the Contracting Party in whose national territory the observation or pursuit is carried out. 7) The Contracting Parties undertake to meet as soon as possible the preconditions for the use by police services of airborne assets in the context of observation or pursuit or in connection with other trans frontier operations decided upon jointly. The Contracting Parties shall inform each other of the fulfilment of these conditions and shall endeavour to extend this possibility to the customs authorities. 8) If the layout of traffic routes so requires, police and customs officers may, in the performance of their duties, travel on the national territory of the neighbouring state until the next opportunity to turn around and return to their own territory. 9) Officers of the police and customs services of the Contracting Parties engaged in a hot pursuit may, when crossing the border, wear their uniforms and carry their service weapons and other means of restraint authorised by their national law. 10) The competent bodies shall exchange information on service weapons and other authorised means of restraint. The use of service weapons shall be permitted only in self-defence. Specific rules for hot pursuit between Spain and France: The same rules as defined under the Schengen acquis apply [Art. 7] Specific rules for hot pursuit between Belgium and France: The same rules as defined under the Schengen acquis apply [Art. 6] Specific rules for hot pursuit between Italy and France: The same rules as defined under the Schengen acquis apply [Art. 8]	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)		
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	General provision When engaging in hot pursuit, the officer of one of the contracting parties who are pursuing in their country an individual caught in the act of committing or participating in one of the offences referred to in [D22] shall be authorised to continue pursuit in the territory of another Contracting Party without the latter's prior authorisation where, given the particular urgency of the situation, it is not possible to notify the competent authorities of the other Contracting Party or where these authorities are unable to reach the scene in time to take over the pursuit.	• Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:42000A0922(02)&from=EN • Agreement with Italy https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000766303?isSuggest=true • Agreement with Switzerland: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000020830546?init=true&isAdvancedResult=true&page=1&pageSize=10&query=%7B%28%40ALL%5Bt%22poursuite+transfrontali%C3%A8re%22%5D%29%7D&tab_selection=all&typeRecherche=date • Agreement with Spain: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000796362?init=true&page=1&query=coop%C3%A9ration+transfrontali%C3%A8re+en+mati%C3%A8re+polici%C3%A8re+et+douani%C3%A8re&searchField=ALL&tab_selection=all • Agreement with the Netherlands: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000031313014?init=true&isAdvancedResult=true&page=1&pageSize=10&query=%7B%28%40ALL%5Bt%22poursuite+transfrontali%C3%A8re%22%5D%29%7D&tab_selection=all&typeRecherche=date • Agreement with Belgium: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000031328288?init=true&isAdvancedResult=true&page=1&pageSize=10&query=%7B%28%40ALL%5Bt%22poursuite+transfrontali%C3%A8re%22%5D%29%7D&tab_selection=all&typeRecherche=date

Relevant items	Provisions	Sources used
		- Agreement with Germany: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000585254?isSuggest=true - Agreement with Luxembourg: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033172518?isSuggest=true - Agreement between Luxembourg, Germany, France and Belgium: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033172518?isSuggest=true
What ongoing supervision is required for the use of this tool?	Applicable to all cases: No specific provision indicates which body is responsible for supervision. However, according to the agreements that France has signed with each of the countries with which it borders, the hot pursuit must be communicated to the joint centres established between France and the other party as soon as the border is crossed. The joint centers will then inform the local authorities.	- Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:42000A0922(02)&from=EN - Agreement with Italy https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000766303?isSuggest=true - Agreement with Switzerland: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000020830546?init=true&isAdvancedResult=true&page=1&pageSize=10&query=%7B%28%40ALL%5Bt%22poursuite+transfrontali%C3%A8re%22%5D%29%7D&tab_selection=all&typeRecherche=date - Agreement with Spain: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000796362?init=true&page=1&query=coop%C3%A9ration+transfrontali%C3%A8re+en+mati%C3%A8re+polici%C3%A8re+et+douani%C3%A8re&searchField=ALL&tab_selection=all - Agreement with the Netherlands: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000031313014?init=true&isAdvancedResult=true&page=1&pageSize=10&query=%7B%28%40ALL%5Bt%22poursuite+transfrontali%C3%A8re%22%5D%29%7D&tab_selection=all&typeRecherche=date - Agreement with Belgium: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000031328288?init=true&isAdvancedResult=true&page=1&pageSize=10&query=%7B%28%40ALL%5Bt%22poursuite+transfrontali%C3%A8re%22%5D%29%7D&tab_selection=all&typeRecherche=date - Agreement with Germany: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000585254?isSuggest=true - Agreement with Luxembourg: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033172518?isSuggest=true - Agreement between Luxembourg, Germany, France and Belgium: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033172518?isSuggest=true
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	The following statutes are applicable when it comes to this investigative tool: - Article 706-57 to Article 706-63 of the Code of Criminal Procedure (Title XXI, Book IV)	Code of Criminal Procedure: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISC_TA000006121328/#LEGISCTA000006121328
How is the tool defined?	The law does not provide a specific definition of the tool. The law states as follows: "[...] Persons against whom there is no plausible reason to suspect that they have committed or attempted to commit an offense and who are likely to provide evidence relevant to the proceedings may, with the authorisation of the district prosecutor or the investigating judge, declare as domicile the address of the police station or the gendarmerie. [...]" [Art. 706-57]	Code of Criminal Procedure: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISC_TA000006121328/#LEGISCTA000006121328
For what types of crime can the tool be used?	cross-crime areas	
Does national law allow this tool to be used in cross-border cases?	The French code of criminal procedure does not provide any specific provisions clarifying whether the tool can be used in the context of cross-border criminal investigations	Code of Criminal Procedure: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISC_TA000006121328/#LEGISCTA000006121328
What thresholds must be passed for the use of this tool?	The tool can be utilised only in the context of an investigation or enquiry into one of the crimes or offences falling within the scope of Article 706-73 and 706-73-1 of the Code of Criminal Procedure: Art. 706-73 and Art. 706-73-1 .	- Art. 706-73 Link: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000035937420 - Art. 706-73-1 Link: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000039183234

Relevant items	Provisions	Sources used
		The penalties applicable to the crimes listed have been retrieved from the Penal Code: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000033975336/
What types of stakeholder are involved in the implementation of this tool?	The following actors are involved in the implementation of the tool Investigating judge and district prosecutor The investigating judge or the district prosecutor are responsible for authorising and supervising the implementation the investigative tool Judge of freedom and liberties In the event of proceedings relating to a felony or an offense punishable by at least three years' imprisonment, when the hearing of the witness is likely to seriously endanger his/her life, members of his/her family or close relations, the judge of freedoms and detention, under request of the district prosecutor or the investigative judge, may authorize that the statements of the witness are collected without his/her identity appearing in the file of the procedure. This decision is not subject to appeal. The liberties and detention judge may decide to proceed with the hearing of the witness himself. [Art. 706-58] National Commission The National Commission for Protection and Rehabilitation is responsible for defining the protective measures that can be granted to witnesses under witness protection.	Code of Criminal Procedure: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISC_TA000006121328/#LEGISCTA000006121328
Which LEAs can use this tool?	LEAs are not mentioned in the articles of the code of criminal procedure relating to "Witness Protection"	
What are the rules to be followed for the implementation of this tool?	The following rules must be respected when using the tool: 1) Witness protection can be used under the authorisation of the district prosecutor or the investigating judge. The authorisation of the district prosecutor is not necessary when the testimony is given by a person holding public authority or entrusted with a public service mission for facts that he has known because of his functions or of his mission.[706-57] 2) The personal address of persons receiving witness protection is entered in a register, opened for this purpose and kept in paper or digital format.[706-57] 3) In the event of proceedings relating to a felony or an offense punishable by at least three years' imprisonment, when the hearing of the witness is likely to seriously endanger his/her life, members of his/her family or close relations, the judge of freedoms and detention, under request of the district prosecutor or the investigative judge, may authorize that the statements of the witness are collected without his/her identity appearing in the file of the procedure. This decision is not subject to appeal. The liberties and detention judge may decide to proceed with the hearing of the witness himself. [Art. 706-58] 4) The decision of the judge of freedoms and detention, which does not reveal the identity of the person, is attached to the report of the witness's hearing, on which the signature of the witness does not appear. The identity and address of the person are entered in another report signed by the witness, which is placed in a file separate from the file of the procedure. The identity and address of the person are entered in a listed and initialled register, which is opened for this purpose in the court. [Art. 706-58] 5) Under no circumstances may the identity or address of a witness having benefited from witness protection be revealed, under specific provisions specified under "6)". [Art. 706-59] 6) The provisions detailed in "3)" are not applicable if, in view of the circumstances in which the offense was committed or the personality of the witness, knowledge of the identity of the person is essential for the exercise of the rights of defense. The indicted person may, within ten days from the date on which he was informed of the content of a hearing of the witness, contest, before the president of the investigative chamber, the information provided by the witness. The president of the investigating chamber, after considering the documentation compiled and the claim made by the accused party, may decide to cancel the hearing or order that the identity of the witness be revealed on condition that the latter expressly makes it known that he/she accepts the lifting of his/her anonymity.[Art. 706-60] 7) The person indicted or referred to the trial court may request to be confronted with a witness under witness protection by means of a technical device allowing the witness to be heard from a distance or to have this witness questioned by his lawyer via the same means. The witness's voice is then rendered unidentifiable by appropriate technical procedures. If the court orders additional information for the purposes of hearing the witness, the latter is heard either by an investigating judge appointed to carry out this additional information, or, if one of the members of the court has been appointed to perform this hearing, using the technical device provided for in the previous paragraph. [Art. 706-61] 8) No conviction may be pronounced on the sole basis of statements collected under the conditions provided for by articles 706-58 ("3)" and "4)") and 706-61 ("7)").[Art. 706-62] 9) In the event of proceedings relating to a crime or an offense punishable by at least three years' imprisonment, when the revelation of the identity of a witness is likely to seriously endanger his or her life or physical integrity or those of his relatives, the investigating judge or the president of the trial court may order, either ex officio or at the request of the district prosecutor or the parties, that this identity not be mentioned during public hearings and does not	Code of Criminal Procedure: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISC_TA000006121328/#LEGISCTA000006121328

Relevant items	Provisions	Sources used
	appear in the orders, judgments or rulings of the investigating or trial court which are likely to be made public. The investigating judge immediately sends a copy of the decision taken to the public prosecutor and to the parties. The decision ordering the confidentiality of the witness's identity is not subject to appeal. The witness is then identified during hearings or judgments by a number assigned to him/her by the investigating judge or the president of the trial court.[Art. 706-62-1] 10) In the event of proceedings relating to a crime or an offence referred to in 706-73 and 706-73-1[D38], where the hearing of a person under witness protection is likely to seriously endanger the life or physical integrity of that person or his or her relatives, that person shall be subject, where necessary, to protective measures designed to ensure his or her safety. Where necessary, he or she may be authorised, under the order of the president of the judicial court, to use an assumed identity. However, such borrowed identity may not be used for a hearing in the proceedings of the case. The protective measures are defined, at the request of the public prosecutor, by the national commission provided for in article 706-63-1[D80]. This commission monitors the protective measures, which it may modify or terminate at any time. In the event of an emergency, the competent services shall take the necessary measures and inform the national commission without delay. Members of the family and relatives of the witness may also be subject to protective measures and be authorised to use a false identity, under the same conditions applicable to the witness.[Art. 706-62-2]	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	1) In the event of proceedings relating to a felony or an offense punishable by at least three years' imprisonment, when the hearing of the witness is likely to seriously endanger his/her life, members of his/her family or close relations, the judge of freedoms and detention, under request of the district prosecutor or the investigative judge, may authorize that the statements of the witness are collected without his/her identity appearing in the file of the procedure. This decision is not subject to appeal. The liberties and detention judge may decide to proceed with the hearing of the witness himself. [Art. 706-58] 2) The provisions detailed in "1)" are not applicable if, in view of the circumstances in which the offense was committed or the personality of the witness, knowledge of the identity of the person is essential for the exercise of the rights of defense. The indicted person may, within ten days from the date on which he was informed of the content of a hearing of the witness, contest, before the president of the investigative chamber, the information provided by the witness. The president of the investigating chamber, after considering the documentation compiled and the claim made by the accused party, may decide to cancel the hearing or order that the identity of the witness be revealed on condition that the latter expressly makes it known that he/she accepts the lifting of his/her anonymity.[Art. 706-60] 3)The person indicted or referred to the trial court may request to be confronted with a witness under witness protection by means of a technical device allowing the witness to be heard from a distance or to have this witness questioned by his lawyer via the same means. The witness's voice is then rendered unidentifiable by appropriate technical procedures. If the court orders additional information for the purposes of hearing the witness, the latter is heard either by an investigating judge appointed to carry out this additional information, or, if one of the members of the court has been appointed to perform this hearing, using the technical device provided for in the previous paragraph. [Art. 706-61] 4) No conviction may be pronounced on the sole basis of statements collected under the conditions provided for by articles 706-58 ("1") and 706-61 ("2").[Art. 706-62]	Code of Criminal Procedure: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISC_TA000006121328/#LEGISCTA000006121328
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	1) Witness protection can be used under the authorisation of the district prosecutor or the investigating judge. The authorisation of the district prosecutor is not necessary when the testimony is given by a person holding public authority or entrusted with a public service mission for facts that he has known because of his functions or of his mission.[706-57] 2) In the event of proceedings relating to a felony or an offense punishable by at least three years' imprisonment, when the hearing of the witness is likely to seriously endanger his/her life, members of his/her family or close relations, the judge of freedoms and detention, under request of the district prosecutor or the investigative judge, may authorize that the statements of the witness are collected without his/her identity appearing in the file of the procedure. This decision is not subject to appeal. The liberties and detention judge may decide to proceed with the hearing of the witness himself. [Art. 706-58] 3) In the event of proceedings relating to a crime or an offence referred to in 706-73 and 706-73-1[D38], where the hearing of a person under witness protection is likely to seriously endanger the life or physical integrity of that person or his or her relatives, that person shall be subject, where necessary, to protective measures designed to ensure his or her safety. Where necessary, he or she may be authorised, under the order of the president of the judicial court, to use an assumed identity.	Code of Criminal Procedure: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISC_TA000006121328/#LEGISCTA000006121328
What ongoing supervision is required for the use of this tool?	The district prosecutor and the investigating judge are in charge of supervising the use of the investigative tool. Additionally, where applicable, the judge of freedom and liberties is responsible	Code of Criminal Procedure: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISC_TA000006121328/#LEGISCTA000006121328

Relevant items	Provisions	Sources used
	for ensuring that the identity of the person under witness protection is protected and not disclosed.	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Surveillance		
Relevant documents (legal and non-legal) that define the functioning of the tool	The general provisions regulating surveillance are provided by Art. 706-80 and Art. 706-81 of the Code of Criminal Procedure. The Code of Criminal Procedure also provides for more specific kinds of surveillance: Wire-tapping: Article 706-95; Bugging: Article 706-96; Data Surveillance: Article 706-102-1 to 706-102-5; Geo-localisation: Article 230-32	- Art. 706-95: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000039279192 - Art. 706-96: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311653 - Art. 706-102-1: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311624 - Art. 230-32: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311484/
Specific range of application of the tool	National legislation regulates the following surveillance activities: - Wire-tapping: Article 706-95 - Collection of technical data and interception of correspondence sent by electronic communications - Article 706-95-20 - Bugging: Article 706-96 - Data Surveillance: Article 706-102-1 to 706-102-5 and Art. 706-95-20 - Geo-localisation: Article 230-32	- Art. 706-95: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000039279192 - Art. 706-96: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311653 - Art. 706-102-1: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311624 - Art. 230-32: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311484/ - Art. 706-95-20: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038270474
How is the tool defined?	The following definitions are provided by the law: Wire-tapping " [...] The recording and transcription of correspondence sent by electronic communications [...]" [Art. 706-95] Collection of technical data and interception of correspondence sent by electronic communications " [...] collect technical connection data enabling the identification of a terminal equipment or the subscription number of its user, as well as data relating to the location of a terminal equipment used. [...]" [Art. 706-95-20] Bugging: "[...] capturing, fixing, transmitting and recording words spoken by one or more persons in a private or confidential capacity, in private or public places or vehicles, or the image of one or more persons in a private place.[...] [Art. 706-96] Data surveillance "[...] accessing, recording, storing and transmitting computer data in any place, as stored in a computer system, as displayed on a screen for the user of an automated data-processing system, as entered by character input or as received and transmitted by peripherals.[...]" [Art. 706-102-01] Geolocalisation "[...] localisation in real time, throughout the national territory, of a person, without his or her knowledge, of a vehicle or any other object, without the consent of its owner or possessor [...]" [Art. 230-32]	- Art. 706-95: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000039279192 - Art. 706-96: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311653 - Art. 706-102-1: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311624 - Art. 230-32: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311484/ - Art. 706-95-20: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038270474
For what types of crime can the tool be used?	Cross crime areas	- Art. 706-73 Link: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000035937420 - Art. 706-73-1 Link: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000039183234
Does national law allow this tool to be used in cross-border cases?	N/A	
What thresholds must be passed for the use of this tool?	The tool can be utilised only in the context of an investigation or enquiry into one of the crimes or offences falling within the scope of Article 706-73 and 706-73-1 of the Code of Criminal Procedure: Art. 706-73 and Art. 706-73-1	- Art. 706-73 Link: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000035937420 - Art. 706-73-1 Link: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000039183234 - The penalties applicable to the crimes listed have been retrieved from the Penal Code: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000033975336/
What types of stakeholder are involved in the implementation of this tool?	The following actors are involved in the context of covert investigations: - District prosecutor (<i>procureur de la République</i>).	Art. 706-95: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000039279192

Relevant items	Provisions	Sources used
	-Liberty and detention judge (juge des libertés et de la détention du tribunal judiciaire) -Investigating judge (<i>juge d'instruction</i>) -Judicial Police Officer (<i>officier de police judiciaire</i>) -Judicial Police Agent (<i>agent de police judiciaire</i>)	• Art. 706-96: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311653 • Art. 706-102-1: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311624 • Art. 230-32: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311484/ • Art. 706-95-20: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038270474
Which LEAs can use this tool?	The following actors can be involved in the utilisation of the tool: Wiretapping -Judicial police officers and agent (under appointment of the investigative judge or district prosecutor, depending on the case) -Any qualified agent of a service placed under the authority of the minister responsible for electronic communications or any qualified agent of an authorised electronic communications network operator (responsible for installing the tool) Bugging, Collection of technical data and interception of correspondence sent by electronic communications, Data surveillance: - Judicial Police Officer appointed by the investigative judge (or judicial police agent under the authority of the judicial police officer) - Any qualified officer from a service, unit or body placed under the authority of the Minister of the Interior or the Minister of Defence. Geolocalisation: - Judicial Police	• Art. 706-95: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000039279192 • Art. 706-96: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311653 • Art. 706-102-1: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311624 • Art. 230-32: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311484/ • Art. 706-95-20: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038270474
What are the rules to be followed for the implementation of this tool?	The following rules must be followed when implementing this tool: General Surveillance: 1) Before engaging in surveillance work, the judicial police officers must inform the district prosecutor in charge of the investigation and the district prosecutor of the jurisdiction where the surveillance is carried out. 2) Judicial police officers must receive authorisation by the district prosecutor in charge of the investigation before requesting any civil servant or public official not to control or arrest people under surveillance. Wiretapping: 1) The investigative tool can only be used in relation to one of the offences falling within the scope of articles 706-73 and 706-73-1 (see D46). [Art. 706-95] 2) Wiretapping must be authorised by the liberty and detention judge upon receiving a request from the district prosecutor. 3) Wiretapping can be used for a maximum of one month (renewable once under the same conditions of form and duration) under the following conditions: - a)The authorisation is in writing and is not subject to appeal. In the case of an offence that is punishable by imprisonment and that has been committed by means of electronic communications on the victim's line, interception may also be authorised (in accordance with the same procedures) if it takes place on that line at the victim's request. [Article 100] b) The decision to authorise interception must state the reasons justifying the use of the investigative tool and the specific legal provisions justifying the necessity to rely on the investigative tool. Additionally, it must state the offence motivating the interception and the duration of the interception. [Article 100-1] c) The investigating judge (or the judicial police officer appointed by him) may require any qualified agent of a body placed under the authority of the minister responsible for electronic communications (or any qualified agent of an authorised electronic communications network operator) to install an interception device [Article 100-3] d) The investigating judge (or the judicial police officer appointed by him) shall draw up a report of each interception and recording operation. This report shall mention the date and time when the operation began and ended. The recordings are placed under closed seals.[Article 100-4] e) The investigating judge (or the judicial police officer appointed by him) transcribes only the correspondence that is relevant to the case and places the transcript in the file of the investigation. Correspondence in a foreign language is transcribed into French with the assistance of an interpreter. Under penalty of nullity, correspondence with a lawyer involved in the exercise of the rights of the defence may not be transcribed. Under penalty of nullity, no correspondence with a journalist which allows a source to be identified in violation of Article 2 of the Law of 29 July 1881 on the freedom of the press may be transcribed.[Article 100-5] f) Once the limitation period for public action has passed, the district prosecutor or the attorney general can order the destruction of the records compiled via the use of the investigative tool. A record is drawn up of the destruction operation.[Article 100-6] g) No interception may take place on the line of a deputy or senator without the president of the assembly to which he or she belongs being informed by the investigating judge. No interception	• Art. 706-95: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000039279192 • Art. 706-96: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311653 • Art. 706-102-1: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311624 • Art. 230-32: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311484/ • Art. 706-95-20: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038270474

Relevant items	Provisions	Sources used
	may take place on a line of a lawyer's firm/home without the President of the Bar being informed by the investigating judge. No interception may take place on a line of the office/home of a magistrate without the first president or the district prosecutor of the jurisdiction where he or she resides being informed.[Article 100-7] h) Where an interception of correspondence sent by electronic communications concerns a communication address which is used on the territory of a Member State of the European Union, and is not carried out in the context of a European investigation order, the investigating judge (or the judicial police officer appointed by him) shall notify the competent authority of that State if the person concerned by the interception is on its territory. Such notification shall take place either before the interception, during or after the interception (as soon as it is established that the person concerned is or was on the territory of that State at the time of the interception). Upon request by the competent authority of the Member State (made within 96 hours of receipt of the notification and justified by the fact that such an interception could not be authorised, in a similar national procedure, under the law of that State) either the interception may not be carried out, must be stopped, or the data intercepted while the person was on its territory may not be used and must be removed from the record of the proceedings. Alternatively, the records may be used only under the conditions and for the reasons specified by that authority. Failure to notify shall constitute a ground for invalidating the proceedings only if it is established that such interception could not have been authorised, in a similar national procedure, under the law of the Member State in whose territory the person was found.[Article 100-8] 4) The liberty and detention judge (or the investigating judge) may authorise, upon request from the district prosecutor, remote access (without knowledge of the person concerned) to correspondence stored by means of electronic communications accessible via a computer identifier. The data to which access has been granted may be entered and recorded (or copied) on any medium. [Art. 706-95-2] 5) The operations mentioned in "4)" are carried out under the authority and control of the magistrate who authorised them and may not, under penalty of nullity, have any purpose other than the investigation into the offences referred to in the decision of the magistrate. [Art. 706-95-3] Common dispositions for Bugging, Collection of technical data and interception of correspondence sent by electronic communications, Data surveillance: 1) These investigative tools may be implemented if the needs of the investigation or judicial enquiry relate to one of the offences listed in D46.[Art.706-95-11] 2) These investigative tools are allowed: a) during the investigation, by the liberty and detention judge at the request of the district prosecutor b) during information, by the investigating judge, upon consulting the district prosecutor. The investigating judge can grant an authorisation without first consulting the district prosecutor only in cases where there is an imminent risk of losing evidence or serious harm to persons or property. In the event of imminent risk, a statement of the factual circumstances establishing the existence of the imminent risk must be submitted. [Art.706-95-12 and 13] 3) The authorisations mentioned in "2)" must be in writing and reference the law justifying the use of the investigative tools. Any rejection of such authorisation cannot be appealed. [Art.706-95-13] 4) If the liberty and custody judge considers that the operations have not been carried out in accordance with his or her authorisation or that the applicable provisions of the Code of Criminal Procedure have not been complied with, he or she shall order the destruction of the reports and recordings made. The judge shall rule by means of an order, which he shall notify to the district prosecutor. The latter may lodge an appeal before the president of the examining magistrate's chamber within ten days of notification. [Art.706-95-14] 5) The authorisation mentioned in "2)a)" has a validity of 1 month, renewable once under the same conditions of form and duration [Art. 706-95-16] 6) The authorisation mentioned in "2)b)" has a validity of 4 months, renewable under the same conditions of form and duration, but the total duration of the operations may not exceed two years. [Art. 706-95-16] 7) These investigative tools can be used by a judicial police officer (appointed by the investigating judge) under request of a district prosecutor [Art. 706-95-17] 8) The district prosecutor, investigating judge or the judicial police officer can request any qualified officer from a service, unit or body under the authority of the Minister of the Interior or the Minister of Defence to install the investigative tools. [Art. 706-95-17] 9) The district prosecutor, the investigating judge or the judicial police officer shall draw up a report on the implementation of the investigative tools . This report shall mention the date and time of beginning and end of the operation. The records shall be kept under sealed cover. The judicial police officer (or the judicial police agent acting under his responsibility) shall describe or transcribe, in a report which shall be placed in the investigation file, the data recorded which are	

Relevant items	Provisions	Sources used
	useful for the case. No sequence relating to private life may be kept in the record of the proceedings. Conversations and data in a foreign language are transcribed into French with the assistance of an interpreter.[Art. 706-95-18] Specific rules for Bugging 1) In the course of the investigation, with a view to setting up the investigative tool, the liberty and detention judge (or the investigating judge, depending on the phase of the investigation) may authorise entry into a vehicle or private property, including outside the hours provided for in Article 59, without the knowledge or consent of the owner or possessor of the vehicle or the occupant of the premises. There operations may have no other purpose than the installation of the technical equipment. The same applies for uninstalling the investigative tool. [706-96-1] 2) This investigative tool cannot be installed in: a) a law firm or at a lawyer's personal address; b) premises of a press or audio-visual communication company c) vehicles, offices or homes of a senator or magistrate [706-96-1] 3) The decision to authorize the use of the investigative tool must include all the elements that facilitate the identification of the vehicles or the private/public places concerned, the offences motivating the use of the tool and the duration of utilisation of the tool. [Art. 706-97] Specific rules for Data collection 1) The district prosecutor or the investigating judge may designate any natural or legal person authorised and registered on one of the lists provided for in Article 157 of the Code of Criminal Procedure to facilitate the utilisation of the investigating tool. The district prosecutor or the investigating judge may also prescribe the use of State resources subject to national defence secrecy. [Art. 706-102-1] 2) The decision to rely on data collection tools must specify the offence motivating the use of the investigative tool, the exact location or detailed description of the automated data processing systems as well as the duration of the operations. [Art. 706-102-3] 3) The installation of the investigative tool into a vehicle or a private property without the knowledge or consent of the owner or possessor of the vehicle (or the occupant of the premises) requires authorisation by the liberty and detention judge, under request of a district prosecutor or of the investigating judge. With a view to setting up the investigative tool, the liberty and detention judge, under request of the district prosecutor, or the investigating judge, may also authorise the transmission of this system via an electronic communications network. [706-102-5] 4) This investigative tool cannot be installed in: a) a law firm or at the lawyer's personal address; b) premises of a press or audio-visual communication company c) vehicles, offices or homes of a senator or magistrate [706-102-5] Specific rules for Geolocalisation: 1) Geolocalisation must be implemented by a judicial police officer (or by a judicial police agent working under his/her responsibility).[Art. 230-32] 2) Geolocalisation can be authorised for a maximum of 15 consecutive days by a district prosecutor. At the end of this delay, an authorisation of a liberty and detention judge (under the request of a district prosecutor) can be obtained for a maximum period of one month, renewable under the same conditions of form and duration. [Art. 230-33] 3) The total duration of the utilisation of geo-localisation cannot exceed 2 years [Art. 230-33] 4) The decision to rely on geo-localisation must specify the offence motivating the use of the investigative tool. Any rejection cannot be appealed. [Art. 230-33] 5) The installation of the investigative tool in private premises intended or used for the storage of vehicles, funds, securities, goods or equipment, (or in a vehicle located on the public highway) without the knowledge or consent of the owner (or occupier of the premises or the vehicle) must be authorised in writing by the district prosecutor or the investigating judge. 6) This investigative tool cannot be installed in: a) a law firm or at the lawyer's personal address; b) premises of a press or audio-visual communication company c) vehicles, offices or homes of a senator or magistrate [Art. 230-34] 7) In case of immediate risk of losing evidence or injury to a person or property, geo-localisation can be implemented directly by a judicial police officer, who is responsible of informing immediately, by any means, the district prosecutor or the investigating judge. However, if entry into a dwelling is necessary, the judicial police officer must obtain prior agreement, given by any means, by the liberty and detention judge. These magistrates have a period of twenty-four hours to prescribe, in writing, the continuation of the operations. If no such authorisation is given within this period, the geolocation shall be terminated. The authorisation shall include a statement of the factual circumstances establishing the existence of the imminent risk.[Art. 230-35]. 8) The investigating judge or the judicial police officer appointed by him or authorised by the district prosecutor may require any qualified member of a service, unit or body placed under the	

Relevant items	Provisions	Sources used
	authority of the Minister of the Interior (and whose list is fixed by decree), to install and remove the investigative tool [Art. 230-36] 9) The judicial police officer (or the judicial police agent acting under his responsibility) shall draw up a report on each of the operations in which geolocalisation has been used. This report shall mention the date and time at which the operation began and the date on which it ended.[Art. 230-38] 10) The judicial police officer or the judicial police agent acting under his or her responsibility shall describe or transcribe, in a report (which shall be placed in the file of the investigation), the recorded data which are useful for the objective of the investigation [Art. 230-39] 11) Where knowledge of certain information is likely to seriously endanger the life or physical integrity of a person, (including members of his or her family or relatives) and that it is neither useful for the case nor indispensable for the exercise of the rights of defence, the judge in charge of liberties and detention may authorise, under request of an investigating judge, that the following information does not appear in the proceedings: a) The date, time and place where tools allowing geolocalisation were installed or removed ; b) The recording of the location data and the elements allowing the identification of a person who has contributed to the installation or removal of geolocalisation tools. The decision of the liberty and detention judge is to be included in the record of the proceedings. The information referred to in a) and b) shall be recorded in another report, which shall be placed in a separate file from the case file, which shall also contain the request of the investigative judge to the liberty and detention judge. This information is entered in a listed and initialled register, which is opened for this purpose at the court of justice.[Art. 230-40] 12) The person under investigation may, within ten days from the date on which he was given knowledge of the content of the geolocation operations contest the use of the tool. If the President of the investigating chamber finds that geolocalisation has been used in an unlawful manner, he/she shall withdraw the authorisation to use the tool[Art. 230-41] 13) Records of location data are destroyed, at the request of the district prosecutor or the attorney general, on expiry of the limitation period for public action. A record is drawn up of the destruction operation.[Art. 230-43] 14) These rules shall not apply where real-time geolocation operations are carried out for the purpose of locating electronic communication terminal equipment, a vehicle or any other object whose owner or lawful possessor the victim of the offence under investigation is. [Art. 230-44]	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Wiretapping: The following restrictions applicable to wiretapping are meant to safeguard individual liberties: 1) The decision to authorise interception must state the reasons justifying the use of the investigative tool and the specific legal provisions justifying the necessity to rely on the investigative tool. Additionally, it must state the offence motivating the interception and the duration of the interception. [Article 100-1] 2) Under penalty of nullity, correspondence with a lawyer involved in the exercise of the rights of the defence may not be transcribed. 3) Under penalty of nullity, no correspondence with a journalist which allows a source to be identified in violation of Article 2 of the Law of 29 July 1881 on the freedom of the press may be transcribed.[Article 100-5] 4) Once the limitation period for public action has passed, the district prosecutor or the attorney general can order the destruction of the records compiled via the use of the investigative tool. A record is drawn up of the destruction operation.[Article 100-6] 5) No interception may take place on the line of a deputy or senator without the president of the assembly to which he or she belongs being informed by the investigating judge. 6) No interception may take place on a line of a lawyer's firm/home without the President of the Bar being informed by the investigating judge. 7) No interception may take place on a line of the office/home of a magistrate without the first president or the district prosecutor of the jurisdiction where he or she resides being informed.[Article 100-7] Common dispositions for Bugging, Collection of technical data and interception of correspondence sent by electronic communications, Data surveillance: The following restrictions applicable to bugging, collection of technical data and interception of correspondence sent by electronic communications, and Data surveillance are meant to safeguard individual liberties: 1) If the liberty and custody judge considers that the operations have not been carried out in accordance with his or her authorisation or that the applicable provisions of the Code of Criminal Procedure have not been complied with, he or she shall order the destruction of the reports and recordings made. The judge shall rule by means of an order, which he shall notify to the district prosecutor. The latter may lodge an appeal before the president of the examining magistrate's chamber within ten days of notification. [Art.706-95-14]	• Art. 706-95: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000039279192 • Art. 706-96: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311653 • Art. 706-102-1: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311624 • Art. 230-32: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311484/ • Art. 706-95-20: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038270474

Relevant items	Provisions	Sources used
	2) No sequence relating to private life may be kept in the record of the proceedings. Conversations and data in a foreign language are transcribed into French with the assistance of an interpreter.[Art. 706-95-18] Specific rules for Bugging meant to safeguard individual liberties: 1) This investigative tool cannot be installed in: a) a law firm or at a lawyer's personal address; b) premises of a press or audio-visual communication company c) vehicles, offices or homes of a senator or magistrate [706-96-1] 2) The decision to authorize the use of the investigative tool must include all the elements that facilitate the identification of the vehicles or the private/public places concerned, the offences motivating the use of the tool and the duration of utilisation of the tool. [Art. 706-97] Specific rules for Data collection meant to safeguard individual liberties: 1) The decision to rely on data collection tools must specify the offence motivating the use of the investigative tool, the exact location or detailed description of the automated data processing systems as well as the duration of the operations. [Art. 706-102-3] 2) The installation of the investigative tool into a vehicle or a private property without the knowledge or consent of the owner or possessor of the vehicle (or the occupant of the premises) requires authorisation by the liberty and detention judge, under request of a district prosecutor or of the investigating judge. With a view to setting up the investigative tool, the liberty and detention judge, under request of the district prosecutor, or the investigating judge, may also authorise the transmission of this system via an electronic communications network. [706-102-5] 3) This investigative tool cannot be installed in: a) a law firm or at the lawyer's personal address; b) premises of a press or audio-visual communication company c) vehicles, offices or homes of a senator or magistrate [706-102-5] Specific rules for Geolocalisation meant to safeguard individual liberties: 1) The installation of the investigative tool in private premises intended or used for the storage of vehicles, funds, securities, goods or equipment, (or in a vehicle located on the public highway) without the knowledge or consent of the owner (or occupier of the premises or the vehicle) must be authorised in writing by the district prosecutor or the investigating judge. 2) This investigative tool cannot be installed in: a) a law firm or at the lawyer's personal address; b) premises of a press or audio-visual communication company c) vehicles, offices or homes of a senator or magistrate [Art. 230-34] 3) Where knowledge of certain information is likely to seriously endanger the life or physical integrity of a person, (including members of his or her family or relatives) and that it is neither useful for the case nor indispensable for the exercise of the rights of defence, the judge in charge of liberties and detention may authorise, under request of an investigating judge, that the following information does not appear in the proceedings: a) The date, time and place where tools allowing geolocalisation were installed or removed; b) The recording of the location data and the elements allowing the identification of a person who has contributed to the installation or removal of geolocalisation tools. 4) The person under investigation may, within ten days from the date on which he was given knowledge of the content of the geolocation operations contest the use of the tool. If the President of the investigating chamber finds that geolocalisation has been used in an unlawful manner, he/she shall withdraw the authorisation to use the tool[Art. 230-41] 5) Records of location data are destroyed, at the request of the district prosecutor or the attorney general, on expiry of the limitation period for public action. A record is drawn up of the destruction operation.[Art. 230-43]	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	General Surveillance: 1) Judicial police officers must receive authorisation by the district prosecutor in charge of the investigation before requesting any civil servant or public official not to carry out controls and arrests of people under surveillance. Wiretapping: 1) Wiretapping must be authorised by the liberty and detention judge upon receiving a request from the district prosecutor [Art. 706-95]. Wiretapping can be used for a maximum of one month (renewable once under the same conditions of form and duration) under the following conditions: a) The authorisation is in writing and is not subject to appeal. [Article 100] b) The decision to authorise the tool must state the reasons justifying the use of the investigative tool and the specific legal provisions justifying the necessity to rely on the investigative tool. Additionally, it must state the offence motivating the interception and the duration of the interception. [Article 100-1] 2) Where an interception of correspondence sent by electronic communications concerns a communication address which is used on the territory of a Member State of the European Union,	• Art. 706-95: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000039279192 • Art. 706-96: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311653 • Art. 706-102-1: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311624 • Art. 230-32: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311484/ • Art. 706-95-20: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038270474

Relevant items	Provisions	Sources used
	and is not carried out in the context of a European investigation order, the investigating judge (or the judicial police officer appointed by him) shall notify the competent authority of that State if the person concerned by the interception is on its territory. Such notification shall take place either before the interception, during or after the interception (as soon as it is established that the person concerned is or was on the territory of that State at the time of the interception). Upon request by the competent authority of the Member State (made within 96 hours of receipt of the notification and justified by the fact that such an interception could not be authorised, in a similar national procedure, under the law of that State) either the interception may not be carried out, must be stopped, or the data intercepted while the person was on its territory may not be used and must be removed from the record of the proceedings. Alternatively, the records may be used only under the conditions and for the reasons specified by that authority. Failure to notify shall constitute a ground for invalidating the proceedings only if it is established that such interception could not have been authorised, in a similar national procedure, under the law of the Member State in whose territory the person was found.[Article 100-8] 3) The liberty and detention judge (or the investigating judge) may authorise, upon request from the district prosecutor, remote access (without knowledge of the person concerned) to correspondence stored by means of electronic communications accessible via a computer identifier. The data to which access has been granted may be entered and recorded (or copied) on any medium. [Art. 706-95-2] Common authorisations for Bugging, Collection of technical data and interception of correspondence sent by electronic communications, Data surveillance: 1) The use of these investigative tools is authorised: a) during the investigation, by the liberty and detention judge at the request of the district prosecutor b) during information, by the investigating judge, upon consulting the district prosecutor. The investigating judge can grant an authorisation without first consulting the district prosecutor only in cases where there is an imminent risk of losing evidence or serious harm to persons or property. In the event of imminent risk, a statement of the factual circumstances establishing the existence of the imminent risk must be submitted. [Art.706-95-12 and 13] 3) The authorisations mentioned in "1)" must be in writing and reference the law justifying the use of the investigative tools. Any rejection of such authorisation cannot be appealed. [Art.706-95-13] 4) If the liberty and custody judge considers that the operations have not been carried out in accordance with his or her authorisation or that the applicable provisions of the Code of Criminal Procedure have not been complied with, he or she shall order the destruction of the reports and recordings made. The judge shall rule by means of an order, which he shall notify to the district prosecutor. The latter may lodge an appeal before the president of the examining magistrate's chamber within ten days of notification. [Art.706-95-14] 5) The authorisation mentioned in "1)a)" has a validity of 1 month, renewable once under the same conditions of form and duration [Art. 706-95-16] 6) The authorisation mentioned in "1)b)" has a validity of 4 months, renewable under the same conditions of form and duration, but the total duration of the operations may not exceed two years. [Art. 706-95-16] Specific authorisations for Bugging 1) In the course of the investigation, with a view to setting up the investigative tool, the liberty and detention judge (or the investigating judge, depending on the phase of the investigation) may authorise entry into a vehicle or private property, including outside the hours provided for in Article 59, without the knowledge or consent of the owner or possessor of the vehicle (or the occupant of the premises). The operations may have no other purpose than the installation of the technical equipment. The same applies for uninstalling the investigative tool. [706-96-1] 2) The decision to authorize the use of the investigative tool must include all the elements that facilitate the identification of the vehicles or the private/public places concerned, the offences motivating the use of the tool and the duration of utilisation of the tool. [Art. 706-97] Specific authorisations for Data collection 1) The district prosecutor or the investigating judge may designate any natural or legal person authorised and registered on one of the lists provided for in Article 157 of the Code of Criminal Procedure to facilitate the utilisation of the investigative tool. The district prosecutor or the investigating judge may also prescribe the use of State resources subject to national defence secrecy. [Art. 706-102-1] 2) The decision to rely on data collection tools must specify the offence motivating the use of the investigative tool, the exact location or detailed description of the automated data processing systems as well as the duration of the operations. [Art. 706-102-3] 3) The installation of the investigative tool into a vehicle or a private property without the knowledge or consent of the owner or possessor of the vehicle (or the occupant of the premises) requires authorisation by the liberty and detention judge, under request of a district prosecutor	

Relevant items	Provisions	Sources used
	or of the investigating judge. With a view to setting up the investigative tool, the liberty and detention judge, under request of the public prosecutor, or the investigating judge, may also authorise the transmission of this system via an electronic communications network. [706-102-5] Specific authorisations for Geolocalisation: 1) Geolocalisation can be authorised for a maximum of 15 consecutive days by a district prosecutor. At the end of this delay, an authorisation of a liberty and detention judge (under the request of a district prosecutor) can be obtained for a maximum period of one month, renewable under the same conditions of form and duration. The total duration of the utilisation of geolocalisation cannot exceed 2 years. The decision to rely on geolocalisation must specify the offence motivating the use of the investigative tool. Any rejection cannot be appealed. [Art. 230-33] 2) The installation of the investigative tool in private premises intended or used for the storage of vehicles, funds, securities, goods or equipment (or in a vehicle located on the public highway or in such premises), without the knowledge or consent of the owner or occupier of the premises or the vehicle must be authorised in writing by the district prosecutor or the investigating judge. 3) In case of immediate risk of losing evidence or injury to a person or property, geolocalisation can be implemented directly by a judicial police officer, who is responsible of informing immediately, by any means, the district prosecutor or the investigating judge. However, if entry into a dwelling is necessary, the judicial police officer must obtain prior agreement, given by any means, by the liberty and detention judge. These magistrates have a period of twenty-four hours to prescribe, in writing, the continuation of the operations. If no such authorisation is given within this period, the geolocation shall be terminated. The authorisation shall include a statement of the factual circumstances establishing the existence of the imminent risk.[Art. 230-35].	
What ongoing supervision is required for the use of this tool?	Wiretapping: Operations involving the use of this investigative tool are supervised by either the liberties and detention judge or the investigative judge. Bugging, Collection of technical data and interception of correspondence sent by electronic communications, Data surveillance: The use of the investigative tools is supervised by the magistrate who has authorised their use (which, can be either the investigative judge or the liberty and detention judge) Geolocalisation The use of the investigative tools is supervised by the magistrate who has authorised their use	• Art. 706-95: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000039279192 • Art. 706-96: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311653 • Art. 706-102-1: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311624 • Art. 230-32: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311484/ • Art. 706-95-20: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038270474
Is there any national case law relating to the use of this tool in cross-border crime cases?	Ruling of 9 May 2018 by the Criminal Division of the Court of Cassation, France Facts of the case: The French authorities had obtained information on the intentions of certain individuals to import cocaine from Peru into French territory. An informant connected the individuals concerned with an undercover agent who had posed as a baggage handler at a Paris airport who could help them smuggle suitcases containing the narcotic products. In an appeal, the defendant in the case pointed out different irregularities concerning the undercover work performed by the government, the use of an informant and geolocalisation [In this section we will only discuss the decision concerning the use of geolocalisation. Please refer to the sections on "Use of informants" and "Undercover operations" to consult the decision of the court on the two other topics]. In the plea, the defendant challenged the rejection by the investigating chamber of the validity of a vehicle's geolocation performed by the police. The irregularity consisted in the lack of prior authorisation by the district prosecutor, contrary to the requirements of Article 230-32 of the Code of Criminal Procedure. The investigating chamber had considered that there was no irregularity insofar as the urgency resulting from the imminent risk of the loss of evidence would have enabled the judicial police officer to set up the system himself, in accordance with Article 230-35 of the Code of Criminal Procedure. Decision The Court of Cassation rejected the investigating chamber's argument stating that "it is not within the powers of the investigating chamber to apply the provisions of the Code where they have not been implemented by the judicial police officer". The authorisation given by the district prosecutor did not mention the geolocation already in place: it was merely an authorisation to implement the measure given on the basis of Article 230-33 and not an authorisation to continue the measure on the basis of Article 230-35. When a judicial police officer uses a geolocalisation tool on his or her own initiative because of the urgency of the situation, the public prosecutor must, within twenty-four hours, order the operations to continue and state the factual circumstances establishing the imminent risk, which was not done in this case.	• Non-legal source providing a summary of the decision: https://www.dalloz-actualite.fr/flash/infiltration-provocation-l-infraction-et-geolocalisation#.YDfkOuhKg2w • Text of the decision: https://www.dalloz-actualite.fr/sites/dalloz-actualite.fr/files/resources/2018/05/17-86.558.pdf

Relevant items	Provisions	Sources used
	In addition to the rejection of the defendant's claim, the investigating chamber had held that the accused could not invoke nullity since he had no right to the vehicle (the geolocalised vehicle belonged to his intimate partner/concubine. On this point, the Court of Cassation overturned the decision because the accused regularly used the geolocalised vehicle. Accordingly, the only cases in which a declaration of invalidity is inadmissible on the grounds of irregularity is when the geolocalised vehicle is stolen or falsely registered. This was not the case here, since the accused was using his concubine's vehicle. He was therefore entitled to claim the invasion of privacy caused by the irregularity of the measure. This case clarified the terms under which geolocalisation can be used by police forces.	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Undercover / covert operations		
Relevant documents (legal and non-legal) that define the functioning of the tool	Art. 706-81 to Art. 706-87 of the Code of Criminal Procedure: Title XXV: On the procedure applicable to organised crime and delinquency and crimes. (De la procédure applicable à la criminalité et à la délinquance organisées et aux crimes)	Link: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISC_TA000006138138/2021-02-25/
How is the tool defined?	"[...] Infiltration consists, for an officer or agent of the judicial police specially authorised under conditions laid down by decree and acting under the responsibility of an officer of the judicial police responsible for coordinating the operation, in monitoring persons suspected of committing a crime or an offence by posing as one of their co-perpetrators, accomplices or receivers to such persons. [...]"	Art. 706-81 of the Code of Criminal Procedure Link: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000031052159
For what types of crime can the tool be used?	"cross crime areas"	- Art. 706-73 Link: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000035937420 - Art. 706-73-1 Link: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000039183234
Does national law allow this tool to be used in cross-border cases?	The French code of criminal procedure does not provide any specific provisions applicable to the implementation of this investigative tool in the context of cross-border operation.	
What thresholds must be passed for the use of this tool?	The tool can be utilised only in the context of an investigation or enquiry into one of the crimes or offences falling within the scope of Article 706-73 and 706-73-1 of the Code of Criminal Procedure: Art. 706-73 and Art. 706-73-1	- Art. 706-73 Link: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000035937420 - Art. 706-73-1 Link: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000039183234 - The penalties applicable to the crimes listed have been retrieved from the Penal Code: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000033975336/
What types of stakeholder are involved in the implementation of this tool?	The following actors are involved in the context of covert investigations: -District prosecutor (<i>procureur de la République</i>): The district prosecutor is responsible for authorising and supervising an undercover operation -Investigating judge (<i>juge d'instruction</i>) Upon receiving the opinion of the district prosecutor, the investigating judge may authorise and supervise an undercover operation. -Judicial Police Officer (<i>officier de police judiciaire</i>) An officer of the judicial police is specially authorised to coordinate the undercover operation and compile a report that includes only the elements that are strictly necessary to establish the offences. The judicial police officer responsible for coordinating the undercover operation can be heard alone as a witness on the operation. -Judicial Police Agent (<i>agent de police judiciaire</i>) The judicial police agent is the person specially authorised to carry-out the undercover operation and authorised to use a false identity. In the context of the undercover operation, the judicial police agent is not held liable for the commission of the following acts: 1. Acquire, hold, transport or deliver substances, goods, products, documents or information derived from or used in the commission of an offence; 2. Using (or providing to persons committing these offences) means of a legal or financial nature as well as means of transport, deposit, accommodation, conservation and telecommunication; 3. Acts committed for the sole purpose of carrying out the undercover operation. If it emerges from the report compiled by the Judicial Police Officer that the person under investigation is directly implicated by observations made by the judicial police agent who personally carried out the undercover operation, that person may ask to be confronted with that agent (under specific conditions).	The actors involved in undercover operations are detailed from Article 706-81 to Art. 706-87 of the Code of Criminal Procedure Link: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISC_TA000006138138/2021-02-25/
Which LEAs can use this tool?	Police Judiciaire. As indicated under article 706-81, infiltrations (or undercover operations) can be conducted by specially authorised officers or agents of the Judicial Police.	Art. 706-81 of the Code of Criminal Procedure Link: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000031052159
What are the rules to be followed for the implementation of this tool?	The following rules must be followed when implementing this tool: 1) The use of this tool must be justified by the needs of the investigation or enquiry into one of the crimes or offences that fall within the scope of Article 706-73 and 706-73-1 [Art. 706-81].	The rules relating to the conduction of undercover operations are detailed from Article 706-81 to Art. 706-87 of the Code of Criminal Procedure. Please refer to the specific references inserted into the text (e.g. [Art. 706-81]) to identify the

Relevant items	Provisions	Sources used
	2) An undercover operation must be authorised by the district prosecutor (<i>procureur de la République</i>) or the investigative judge (upon receiving the opinion of the district prosecutor).[Art. 706-81] 3) The undercover operation can be conducted by an agent of the judicial police who is specially authorised to conduct this type of operations.[Art. 706-81] 4) The report compiled by the officer of the judicial police responsible for coordination the undercover operation must include only the elements strictly necessary to establish the offences and which do not endanger the security of the undercover agent.[Art. 706-81] 5) The judicial police agent is authorised to use a false identity [Art. 706-81] and is not held liable for the commission of the following acts: a. Acquire, hold, transport or deliver substances, goods, products, documents or information derived from or used in the commission of an offence; b. Using (or providing to persons committing these offences) means of a legal or financial nature as well as means of transport, deposit, accommodation, conservation and telecommunication; c. Acts committed for the sole purpose of carrying out the undercover operation.[Art. 706-82] 6) The authorisation mentioned in "1)" must be issued in writing and must be specially motivated. It shall mention the offence(s) justifying recourse to this procedure and the identity of the judicial police officer under whose responsibility the operation is carried out. [Art. 706-83] 7) The authorisation sets the duration of the undercover operation, which may not exceed four months. The operation may be renewed under the same conditions of form and duration. The magistrate who authorised the operation may, at any time, order its interruption before the expiry of the fixed duration. [Art. 706-83] 8) The authorisation shall be entered in the case file after completion of the undercover operation. [Art. 706-83] 9) The real identity of the officers or agents of the judicial police who carried out the infiltration under an assumed identity must not appear at any stage of the procedure. [Art. 706-84] 10) In the event of a decision to interrupt the operation (or at the end of the time limit set by the decision authorising the infiltration and in the absence of an extension), the undercover agent may continue the activities mentioned in "5)", without being criminally liable, for the time strictly necessary to enable him to cease his surveillance in conditions ensuring his safety, without this period exceeding four months. In this case, the magistrate who issued the authorisation shall be informed as soon as possible. If, at the end of the four-month period, the undercover agent cannot cease his operation under conditions ensuring his safety, the magistrate shall authorise its extension for a maximum period of four months. [Art. 706-85] 11) The judicial police officer under whose responsibility the undercover operation takes place can be heard alone as a witness on the operation. However, if it emerges from the report compiled by the judicial police officer that the person under investigation (or appearing before the court) is directly implicated by observations made by an officer who personally carried out the undercover operations, that person may ask to be confronted with that officer (under specific conditions). The questions put to the undercover agent on the occasion of this confrontation must not have the object or effect of revealing, directly or indirectly, his true identity.[Art. 706-86] 12) No conviction may be pronounced solely on the basis of statements made by officers or agents of the judicial police who have carried out an undercover operation. [Art. 706-87]	information provided in the text of the law. Link: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISC_TA000006138138/2021-02-25/
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	1) The use of this tool must be justified by the needs of the investigation or enquiry into one of the crimes or offences that fall within the scope of Article 706-73 and 706-73-1 [Art. 706-81]. 2) The judicial police officer under whose responsibility the undercover operation takes place can be heard alone as a witness on the operation. However, if it emerges from the report compiled by the judicial police officer that the person under investigation (or appearing before the court) is directly implicated by observations made by an officer who personally carried out the undercover operations, that person may ask to be confronted with that officer (under specific conditions). The questions put to the undercover agent on the occasion of this confrontation must not have the object or effect of revealing, directly or indirectly, his true identity.[Art. 706-86] 3) No conviction may be pronounced solely on the basis of statements made by officers or agents of the judicial police who have carried out an undercover operation. [Art. 706-87]	The rules relating to the conduction of undercover operations are detailed from Article 706-81 to Art. 706-87 of the Code of Criminal Procedure. Please refer to the specific references inserted into the text (e.g. [Art. 706-81]) to identify the information provided in the text of the law. Link: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISC_TA000006138138/2021-02-25/
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	An undercover operation must be authorised by the district prosecutor (<i>procureur de la République</i>) or the investigative judge (upon receiving the opinion of the district prosecutor)[Art. 706-81]. The authorisation must be issued in writing and must be specially motivated. It shall mention the offence(s) justifying recourse to this procedure and the identity of the judicial police officer under whose responsibility the operation is carried out [Art. 706-83]. The authorisation sets the duration of the undercover operation, which may not exceed four months. The operation may be renewed under the same conditions of form and duration. The magistrate who authorised the operation may, at any time, order its interruption before the expiry of the fixed duration. [Art. 706-84]	The rules relating to the authorisation of an undercover operations are detailed from Article 706-81 to Art. 706-87 of the Code of Criminal Procedure. Link: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISC_TA000006138138/2021-02-25/

Relevant items	Provisions	Sources used
	In the event of a decision to interrupt the operation (or at the end of the time limit set by the decision authorising the infiltration and in the absence of an extension), the undercover agent may continue the activities mentioned in "5)" (D60), without being criminally liable, for the time strictly necessary to enable him to cease his surveillance in conditions ensuring his safety, without this period exceeding four months. In this case, the magistrate who issued the authorisation shall be informed as soon as possible. If, at the end of the four-month period, the undercover agent cannot cease his operation under conditions ensuring his safety, the magistrate shall authorise its extension for a maximum period of four months.[Art. 706-85] The authorisation shall be entered in the case file after completion of the undercover operation. [Art. 706-83]	
What ongoing supervision is required for the use of this tool?	The use of the tool is to be supervised by the district prosecutor (or the investigative judge - upon receipt of an opinion by the district prosecutor). The conduction of the undercover operation is to be coordinate by a judicial police officer, who is also responsible for compiling a report of the operation.	The rules relating to the supervision of an undercover operations are detailed from Article 706-81 to Art. 706-87 of the Code of Criminal Procedure. Link: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISC_TA000006138138/2021-02-25/
Is there any national case law relating to the use of this tool in cross-border crime cases?	Ruling of 9 May 2018 by the Criminal Division of the Court of Cassation, France Facts of the case: The French authorities had obtained information on the intentions of certain individuals to import cocaine from Peru into French territory. An informant connected the individuals concerned with an undercover agent who had posed as a baggage handler at a Paris airport who could help them smuggle suitcases containing the narcotic products. According to the appeal submitted by the defendant in the case, the rules governing undercover work were not respected. More specifically, the defendant held that: 1. the informant had himself been infiltrated without having been authorised to do so under the terms of the law. According to Article 706-81 of the Code of Criminal Procedure, undercover operations must be authorised by the district prosecutor during the investigation or by the investigating judge during a judicial investigation. In the case, the district prosecutor had only authorised the infiltration of the agent posing as a baggage handler and not the informant. 2. The appellant also challenged the fairness of the evidence gathered as a result of the infiltration. He maintained that the informant had provoked the offence because, without the contact with the undercover agent who was planning to take the luggage through the airport, the offence of importing narcotic products could not have been committed. Decision of the Court of Cassation: Decisions of the court in relation to the two arguments raised by the defendant: 1. The Court of Cassation simply noted that the informant was not an undercover agent inasmuch as he merely put the perpetrators and the undercover agent in contact with each other. According to the Court, this statement alone does not seem sufficient to be convincing, as it is not known how the informant had the necessary credibility with the persons concerned to put them in touch with a baggage handler who was likely to let suitcases full of narcotics through at Roissy airport. 2. the Court of Cassation stated that the informant "merely put in touch with this service a team of traffickers operating from Peru and wishing to import cocaine into France, looking for a baggage handler to take the proceeds out of the airport[.]". The undercover agent had simply responded to the request, made by the traffickers, to receive the proceeds on arrival on national territory. "[..] Neither the informant nor the undercover agent had provoked the commission of the offence". This decision clarified what constitutes a legitimate use of undercover operations as an investigative tool and when it does not constitute entrapment.	- Non-legal source providing a summary of the decision: https://www.dalloz-actualite.fr/flash/infiltration-provocation-l-infraction-et-geolocalisation#.YDfkOuhKg2w - Text of the decision: https://www.dalloz-actualite.fr/sites/dalloz-actualite.fr/files/resources/2018/05/17-86.558.pdf
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	- Code of Criminal Procedure: Titre XXI bis : Protection of persons benefiting from exemptions or reductions in penalties for preventing the commission of offences, halting or mitigating the damage caused by an offence, or identifying the perpetrators or accomplices of offences (<i>Protection des personnes bénéficiant d'exemptions ou de réductions de peines pour avoir permis d'éviter la réalisation d'infractions, de faire cesser ou d'atténuer le dommage causé par une infraction, ou d'identifier les auteurs ou complices d'infractions</i>) (Articles 706-63-1 à 706-63-2) - Decree no. 2014-346 of 17 March 2014 relating to the protection of persons mentioned in articles 706-62-2 and 706-63-1 of the code of criminal procedure (<i>Décret n° 2014-346 du 17 mars 2014 relatif à la protection des personnes mentionnées aux articles 706-62-</i>	- Code of criminal procedure: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000039279254/ - Decree no. 2014-346 of 17 March 2014 relating to the protection of persons mentioned in articles 706-62-2 and 706-63-1 of the code of criminal procedure: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000028745334/

Relevant items	Provisions	Sources used
	<i>2 et 706-63-1 du code de procédure pénale</i>), which provides specific provisions for the use of a false identity by informants.	
Specific range of application of the tool	As per Article 132-78 of the French penal code, an informant is "[...] A person who has attempted to commit a crime or misdemeanour [that] is, in the cases provided for by law, exempt from punishment if, having notified the administrative or judicial authority, he or she has prevented the commission of the offence and, where appropriate, has helped to identify the other perpetrators or accomplices.[...]". Therefore, based on national legislation, informants are members of an organised criminal group . Additionally, according to article 706-63-1 of the Code of Criminal Procedure, all the provisions applicable to informants are also applicable to their relatives and family members.	- Code of criminal procedure: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000039279254/ - Decree no. 2014-346 of 17 March 2014 relating to the protection of persons mentioned in articles 706-62-2 and 706-63-1 of the code of criminal procedure: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000028745334/
How is the tool defined?	As per Article 132-78 of the French penal code, an informant is "[...] A person who has attempted to commit a crime or misdemeanour [that] is, in the cases provided for by law, exempt from punishment if, having notified the administrative or judicial authority, he or she has prevented the commission of the offence and, where appropriate, has helped to identify the other perpetrators or accomplices.[...]".	Code of criminal procedure: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000039279254/
For what types of crime can the tool be used?	The code of criminal procedure refers to informant as someone who has prevented the commission of a <i>crime ou délit</i> . According to the ministry of the interior, a crime is punishable by a minimum of 15 years to life in prison, while a <i>délit</i> is punishable from a minimum of 2 months to a maximum of 10 years. Therefore "cross crime areas".	- Code of criminal procedure: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000039279254/ - Decree no. 2014-346 of 17 March 2014 relating to the protection of persons mentioned in articles 706-62-2 and 706-63-1 of the code of criminal procedure: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000028745334/ - Ministry of the Interior: https://www.demarches.interieur.gouv.fr/particuliers/quelles-differences-entre-contravention-delit-crime
Does national law allow this tool to be used in cross-border cases?	The French Code of Criminal Procedure does not provide any specific provisions specifying whether the investigative tool can be used in the context of cross-border investigations.	
What thresholds must be passed for the use of this tool?	The code of criminal procedure refers to informant as someone who has prevented the commission of a <i>crime ou délit</i> . According to the ministry of the interior, a crime is punishable by a minimum of 15 years to life in prison, while a <i>délit</i> is punishable from a minimum of 2 months to a maximum of 10 years. Therefore "cross crime areas".	- Code of criminal procedure: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000039279254/ - Decree no. 2014-346 of 17 March 2014 relating to the protection of persons mentioned in articles 706-62-2 and 706-63-1 of the code of criminal procedure: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000028745334/ - Ministry of the Interior: https://www.demarches.interieur.gouv.fr/particuliers/quelles-differences-entre-contravention-delit-crime
What types of stakeholder are involved in the implementation of this tool?	The following actors are involved in the implementation of the tool: 1) The National Commission for Protection and Rehabilitation, placed under the authority of the Minister of the Interior. This commission sets the obligations to be respected by the informant and monitors protection and reintegration measures, which it can modify or terminate at any time. It is composed of: - a magistrate active or honorary appointed by the Minister of Justice - two magistrates working or having worked in a specialised inter-regional court, appointed by the Minister of Justice - one magistrate representing the Department of Criminal Affairs and Pardons - a representative of the general directorate of the national police force - a representative of the Directorate General of Internal Security - a representative of the general directorate of the national gendarmerie - a representative of the minister in charge of customs It also includes, in an advisory capacity, a representative of the inter-ministerial technical assistance service at the Ministry of the Interior. The members of the commission, as well as their alternates, are appointed for a period of three years, renewable once, by joint order of the Minister of Justice, the Minister of the Interior and the Minister in charge of customs. 2) The President of the Paris Court of Justice Responsible to authorise any requests to use a false identity. 3) Inter-ministerial technical assistance service Only authority responsible for creating false identities, storing them in a database and reconciling them with real identities. 4) Judicial Police and gendarmerie [Art.15-1] The police and gendarmerie services may pay compensation to any person not belonging to the public administrations who has provided them with information that has directly led either to the discovery of crimes or misdemeanours or to the identification of the perpetrators of crimes or misdemeanours. 5) Customs	- Decree no. 2014-346 of 17 March 2014 relating to the protection of persons mentioned in articles 706-62-2 and 706-63-1 of the code of criminal procedure: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000028745334/ - Art. 15-1 of the Law No. 95-73 of 21 January 1995 on security orientation and programming (<i>Loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité</i>): https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000006527963/2004-03-10 - Assessing Measures Against Organised Crime (AMOC). 2015. Study on paving the way for future policy initiatives in the field of fight against organised crime - effectiveness of specific criminal law measures targeting organised crime. Section 3. (Link unavailable)

Relevant items	Provisions	Sources used
	Customs are authorised to use and pay informants under the same conditions as the police. (confirmed by AMOC - see sources)	
Which LEAs can use this tool?	The following LEAs are allowed to use the tool: 1) Judicial police and gendarmerie 2) Customs	Art. 15-1 of the Law No. 95-73 of 21 January 1995 on security orientation and programming (Loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité): https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000006527963/2004-03-10
What are the rules to be followed for the implementation of this tool?	The following rules apply when implementing the tool: 1) The National Commission for Protection and Rehabilitation analyses the requests to rely on an informant that are submitted by the district prosecutor in charge of the case or, where appropriate, by the investigating judge who notifies the prosecutor. A copy of the application and the accompanying documents are placed in a separate file from the file of the proceedings. This file is kept by the district prosecutor 2) As soon as the request is received, the chairman of the commission requests the inter-ministerial technical assistance service to investigate it. To this end: - the persons concerned by the measures may be heard at any time ; - all persons useful to the commission's mission may be requested and all useful supporting documents may be requested; - the district prosecutor or the investigating judge may be asked for additional information. 3) The inter-ministerial technical assistance service reports on its instruction to the president of the commission. The latter rejects requests that do not meet the conditions relating to the scope of the law. 4) The President of the Paris Court of Justice is responsible for authorising any requests to use a false identity. 5) The President of the Court may decide to hear the person who has requested to use a false identity. This hearing is not public. No minutes can be drawn up. The order issued by the President of the Court is not made public and shall be notified to the chairman of the National Commission for Protection and Rehabilitation and to the person concerned by any means. A copy of the order shall be kept at the registry. 6) In the event of criminal proceedings against a person using a false identity, that person shall be sentenced under his/her false identity. The conviction is entered in the criminal record under the false identity. If the authorisation to use a false identity is withdrawn, the person is sentenced under his or her real identity (if the withdrawal takes place before the sentence is passed). If the person has previously been convicted under his or her false identity, the district prosecutor at the Paris criminal court requires the criminal record to record these convictions under the real identity and to delete any reference to the false identity.	Decree no. 2014-346 of 17 March 2014 relating to the protection of persons mentioned in articles 706-62-2 and 706-63-1 of the code of criminal procedure: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000028745334/
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	None could be identified	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	The following authorisations are needed prior to engaging an informant: 1) The National Commission for Protection and Rehabilitation decides (under the opinion of the "inter-ministerial technical assistance service") on any requests concerning potential protection and reintegration measures for informants (and their families). 2) The President of the Paris Court of Justice is responsible for authorising the use of a false identity by an informant.	Decree no. 2014-346 of 17 March 2014 relating to the protection of persons mentioned in articles 706-62-2 and 706-63-1 of the code of criminal procedure: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000028745334/
What ongoing supervision is required for the use of this tool?	1) The National Commission for Protection and Rehabilitation 2) The President of the Paris Court of Justice	Decree no. 2014-346 of 17 March 2014 relating to the protection of persons mentioned in articles 706-62-2 and 706-63-1 of the code of criminal procedure: https://www.legifrance.gouv.fr/loda/id/JORFTEXT000028745334/
Is there any national case law relating to the use of this tool in cross-border crime cases?	Ruling of 9 May 2018 by the Criminal Division of the Court of Cassation, France Facts of the case: The French authorities had obtained information on the intentions of certain individuals to import cocaine from Peru into French territory. An informant connected the perpetrators concerned with an undercover agent who had posed as a baggage handler at a Paris airport who could help them smuggle suitcases containing the narcotic products. According to the appeal submitted by the defendant in the case, the rules governing undercover work were not respected. More specifically, the defendant held that: 1. the informant had himself been infiltrated without having been authorised to do so under the terms of the law. According to Article 706-81 of the Code of Criminal Procedure, undercover operations must be authorised by the district prosecutor during the investigation or by the investigating judge during a judicial investigation.	- Non-legal source providing a summary of the decision: https://www.dalloz-actualite.fr/flash/infiltration-provocation-l-infraction-et-geolocalisation#.YDfkOuhKg2w - Text of the decision: https://www.dalloz-actualite.fr/sites/dalloz-actualite.fr/files/resources/2018/05/17-86.558.pdf

Relevant items	Provisions	Sources used
	In the case, the district prosecutor had only authorised the infiltration of the agent posing as a baggage handler and not the informant. 2. The appellant also challenged the fairness of the evidence gathered as a result of the infiltration. He maintained that the informant had provoked the offence because, without the contact with the undercover agent who was planning to take the luggage through the airport, the offence of importing narcotic products could not have been committed. Decision of the Court of Cassation: Decisions of the court in relation to the two arguments raised by the defendant: 1. The Court of Cassation simply noted that the informant was not an undercover agent inasmuch as he merely put the perpetrators and the undercover agent in contact with each other. This statement alone does not seem sufficient to be convincing, as it is not known how the informant had the necessary credibility with the persons concerned to put them in touch with a baggage handler who was likely to let suitcases full of narcotics through at Roissy airport. 2. the Court of Cassation stated that the informant "merely put in touch with this service a team of traffickers operating from Peru and wishing to import cocaine into France, looking for a baggage handler to take the proceeds out of the airport[...]" The undercover agent had simply responded to the request, made by the traffickers, to receive the proceeds on arrival on national territory. "[...] Neither the informant nor the undercover agent had provoked the commission of the offence". This decision clarifies the definition of informant and under what conditions an individual can be considered to be an informant.	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Criminal analysis - Judicial Reconciliation (Rapprochement Judiciaire)		
Relevant documents (legal and non-legal) that define the functioning of the tool	The following statutes are applicable when it comes to this investigative tool: -Art. 230-20 to 27, Chapter II of the Code of Criminal Procedure (Software for judicial reconciliation - <i>Des logiciels de rapprochement judiciaire</i>) -Decree no. 2012-687 of 7 May 2012 relating to the implementation of software for judicial reconciliation for the purpose of criminal analysis (this decree provides specific provisions for the utilisation of software for judicial reconciliation) -Deliberation No. 2011-418 of 15 December 2011 providing an opinion on a draft decree relating to the implementation of judicial reconciliation software for criminal analysis purposes (request for opinion No. 1523917 (document providing contextual information on the implementation of the software AnaCrim described in this section))	- Code of Criminal Procedure, Chapter III, Articles 230-20 to 230-27: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISC_TA000023710126/2021-03-03/ - Deliberation No. 2011-418 of 15 December 2011 providing an opinion on a draft decree relating to the implementation of judicial reconciliation software for criminal analysis purposes (request for opinion No. 1523917: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000025826039 - Decree no. 2012-687 of 7 May 2012 relating to the implementation of software for judicial reconciliation for the purpose of criminal analysis: https://www.legifrance.gouv.fr/loda/id/LEGITEXT000025879033/
How is the tool defined?	The code of criminal procedure provides a legal basis for the performance of criminal analysis via the use of software, but it does not provide a definition of the tools currently being used in the context of criminal investigations. The software used for criminal analysis are: 1) AnaCrim ATRT (<i>Application de Traitement des Relations Transactionnelles</i> - Transactional Relationship Processing Application) The software is used in the context of criminal analysis by the French gendarmerie. The ANACRIM-ATRT software enables the automated processing of bank statements and telephone documents (detailed invoicing, relay location, etc.), obtained on judicial requisitions. Through its data search, sorting and cross-checking functions, the application enables the investigator to highlight correlations between the data collected. 2) ANACRIM-ANB (Analysa NoteBook) ANACRIM-ANB is a software for the analysis and visual representation of data. It enables data to be represented in the form of relational or event-based graphs, in order to represent, for example, networks of relationships between individuals or chronological sequences of events. The information contained in procedural documents and documents (minutes, reports, etc.) is thus represented in different forms, which can be enriched by the investigators in order to highlight contradictions between certain data or to confirm certain facts.	- Code of Criminal Procedure, Chapter III, Articles 230-20 to 230-27: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISC_TA000023710126/2021-03-03/ - Deliberation No. 2011-418 of 15 December 2011 providing an opinion on a draft decree relating to the implementation of judicial reconciliation software for criminal analysis purposes (request for opinion No. 1523917: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000025826039 - Decree no. 2012-687 of 7 May 2012 relating to the implementation of software for judicial reconciliation for the purpose of criminal analysis: https://www.legifrance.gouv.fr/loda/id/LEGITEXT000025879033/
For what types of crime can the tool be used?	The software can be used in the context of investigations of <i>flagrante delicto</i> or preliminary investigations and investigations relating to crimes and offences punishable by imprisonment. Therefore: "cross crime areas"	Deliberation No. 2011-418 of 15 December 2011 providing an opinion on a draft decree relating to the implementation of judicial reconciliation software for criminal analysis purposes (request for opinion No. 1523917: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000025826039
Does national law allow this tool to be used in cross-border cases?	N/A	
What thresholds must be passed for the use of this tool?	The software can be used in the context of investigations of <i>flagrante delicto</i> or preliminary investigations and investigations relating to crimes and offences punishable by imprisonment.	Decree no. 2012-687 of 7 May 2012 relating to the implementation of software for judicial reconciliation for the purpose of criminal analysis: https://www.legifrance.gouv.fr/loda/id/LEGITEXT000025879033/

Relevant items	Provisions	Sources used
What types of stakeholder are involved in the implementation of this tool?	- Members of the Judicial Police and of the Gendarmerie, specially trained to use the tool - District Prosecutor (in charge of the management of the personal data used for reconciliation) - Investigating judge - A Magistrate responsible for supervising the implementation of the tool and ensuring the update of the information utilised. The magistrate is appointed for this task by the Ministry of Justice. The implementation of the software is authorised by the magistrate hearing the case or in charge of the investigation. The members of the Judicial Police and of the Gendarmerie who use the tools are subject to an authorisation by either one of the following: - the heads of the territorial services of the national police - the heads of the active services at the prefecture of police - the prefect of police - the heads of the central services of the national police or, where appropriate, the director general of the national police.	• Decree no. 2012-687 of 7 May 2012 relating to the implementation of software for judicial reconciliation for the purpose of criminal analysis: https://www.legifrance.gouv.fr/loda/id/LEGITEXT000025879033/
Which LEAs can use this tool?	- Members of the Judicial Police and of the Gendarmerie, specially trained to use the tool - District Prosecutor (in charge of the management of the personal data used for reconciliation) - Investigating judge - A Magistrate responsible for supervising the implementation of the tool and ensuring the update of the information utilised. The magistrate is appointed for this task by the Ministry of Justice.	• Code of Criminal Procedure, Chapter III, Articles 230-20 to 230-27: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISC_TA000023710126/2021-03-03/ • Decree no. 2012-687 of 7 May 2012 relating to the implementation of software for judicial reconciliation for the purpose of criminal analysis: https://www.legifrance.gouv.fr/loda/id/LEGITEXT000025879033/
What are the rules to be followed for the implementation of this tool?	The following rules must be followed when using the software for criminal analysis: 1) Personal data and information used by the software may only be obtained from the documents and records of legal proceedings already in possession of the authorities authorised to use the tool [Art. 2, Decree no.2012-687 AND Art. 230-21 of the Code of Criminal Procedure] 2) The personal data and information used for reconciliation are accessible to the persons referred to officers and agents of the judicial police and gendarmerie, investigating judge and district prosecutor, and the magistrate supervising the use of the tool. [Art. 3, Decree no.2012-687 AND Art. 230-25 of the Code of Criminal Procedure] 3) These data and information may be sent to the following recipients: a) Officers and agents of the criminal investigation department of the national police and gendarmerie b) International judicial police cooperation bodies and foreign police services (under the conditions set in Art.24 of the law of 18 March 2003)[Art. 3, Decree no.2012-687] 4) Any use of the software must be recorded by specifying the identifier of the person who has used the software along with the date and time of the consultation. These data are kept for five years. [Art. 4, Decree no.2012-687] 5) Under no circumstances may the software be used for the purposes of administrative surveys, nor for any other purpose than in the ones specified in the code of criminal procedure [Art. 230-26 of the Code of Criminal Procedure]	• Code of Criminal Procedure, Chapter III, Articles 230-20 to 230-27: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISC_TA000023710126/2021-03-03/ • Decree no. 2012-687 of 7 May 2012 relating to the implementation of software for judicial reconciliation for the purpose of criminal analysis: https://www.legifrance.gouv.fr/loda/id/LEGITEXT000025879033/
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	1) Personal data and information used by the software may only be obtained from the documents and records of legal proceedings already in possession of the authorities authorised to use the tool [Art. 2, Decree no.2012-687 AND Art. 230-21 of the Code of Criminal Procedure] 2) The personal data and information used for reconciliation are accessible to the persons referred to officers and agents of the judicial police and gendarmerie, investigating judge and district prosecutor, and the magistrate supervising the use of the tool. [Art. 3, Decree no.2012-687 AND Art. 230-25 of the Code of Criminal Procedure] 3) These data and information may be sent to the following recipients: a) Officers and agents of the criminal investigation department of the national police and gendarmerie b) International judicial police cooperation bodies and foreign police services (under the conditions set in Art.24 of the law of 18 March 2003)[Art. 3, Decree no.2012-687] 4) Under no circumstances may the software be used for the purposes of administrative surveys, nor for any other purpose than in the ones specified in the code of criminal procedure [Art. 230-26 of the Code of Criminal Procedure]	• Code of Criminal Procedure, Chapter III, Articles 230-20 to 230-27: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISC_TA000023710126/2021-03-03/ • Decree no. 2012-687 of 7 May 2012 relating to the implementation of software for judicial reconciliation for the purpose of criminal analysis: https://www.legifrance.gouv.fr/loda/id/LEGITEXT000025879033/
What authorisation is needed for the use of this tool?(e.g. senior police officer, prosecutor, judge, other)	Applicable to both tools 1) Personal data and information used by the software may only be obtained from the documents and records of legal proceedings already in possession of the authorities authorised to use the tool [Art. 2, Decree no.2012-687 AND Art. 230-21 of the Code of Criminal Procedure] 2) The police and judicial bodies using the tool are specially authorised to use it.	• Code of Criminal Procedure, Chapter III, Articles 230-20 to 230-27: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISC_TA000023710126/2021-03-03/ • Decree no. 2012-687 of 7 May 2012 relating to the implementation of software for judicial reconciliation for the purpose of criminal analysis: https://www.legifrance.gouv.fr/loda/id/LEGITEXT000025879033/
What ongoing supervision is required for the use of this tool?	The use of the software is supervised by a magistrate appointed for this task by the Ministry of Justice	• Code of Criminal Procedure, Chapter III, Articles 230-20 to 230-27: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISC_TA000023710126/2021-03-03/

Relevant items	Provisions	Sources used
	The magistrate supervises the implementation of the software and ensures that the data is kept up to date. He may act on his own initiative and has a direct access to the software in order to carry out his or her duties.[Art. 230-24]	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	

Source: Author's own elaboration

Germany

Table 28 – Overview of national rules on investigative tools - Germany

Relevant items	Provisions	Sources used
Controlled Delivery		
Relevant documents (legal and non-legal) that define the functioning of the tool	Controlled delivery is not governed by law in Germany. In practice, it is subject to the tactical discretion of the criminal prosecution authorities. Individual provisions can be found in guidelines issued to the criminal prosecution office, which is the authority in charge of the investigation proceedings. The police must follow the instructions of the office (§161 and §163 of the Code of Criminal Procedure [StPO])	https://www.unafei.or.jp/publications/pdf/RS_No58/No58_10VE_Hilger1.pdf §161 StPO: https://dejure.org/gesetze/StPO/161.html §163 StPO: https://dejure.org/gesetze/StPO/163.html
How is the tool defined?	Controlled delivery is a tool employed by the criminal prosecution authorities which is indispensable to effectively detect international organised crime. In Germany, it is defined as controlled importation, controlled exportation and controlled transit. [if not governed by law, where is this definition taken from exactly?-according to who is it indispensable?] JMA: this definition is taken from the source of the right column. Author of the source is Johan Peter Wilhelm Hilger, Former Head of Division of Judicial System, Federal Ministry of Justice in Germany.	https://www.unafei.or.jp/publications/pdf/RS_No58/No58_10VE_Hilger1.pdf
For what types of crime can the tool be used?	Controlled delivery is the illegal transportation of narcotics, arms, stolen goods and property, etc. [if you have this information it would be useful to know which ones are covered under etc.] JMA: This information is not given in the consulted source of the right column - no further information identified to clarify your question, from a foreign country through domestic territory to a third country, monitored by the criminal prosecution authorities.	https://www.unafei.or.jp/publications/pdf/RS_No58/No58_10VE_Hilger1.pdf
Does national law allow this tool to be used in cross border cases?	no further information identified	no further information identified
What thresholds must be passed for the use of this tool?	The criminal prosecution authorities are obliged to initiate the measures necessary for prosecution without delay, in particular to solve the crime, when they gain knowledge or form a suspicion of the commission of a criminal offence. Furthermore, the duty to act 'within a reasonable time', as prescribed in Article 6 part 1 of the European Human Rights Convention, applies in Germany. This means that the necessary criminal prosecution measures are to be taken without delay. No further information identified for the maximum term of imprisonment of crimes for which the tool can be used.	https://www.unafei.or.jp/publications/pdf/RS_No58/No58_10VE_Hilger1.pdf
What types of stakeholder are involved in the implementation of this tool?	The implementation of the tool is subject to the tactical discretion of the criminal prosecution authorities.	https://www.unafei.or.jp/publications/pdf/RS_No58/No58_10VE_Hilger1.pdf
Which LEAs can use this tool?	The police must follow the instructions of the prosecution office.	https://www.unafei.or.jp/publications/pdf/RS_No58/No58_10VE_Hilger1.pdf §161 StPO: https://dejure.org/gesetze/StPO/161.html §163 StPO: https://dejure.org/gesetze/StPO/163.html https://www.unafei.or.jp/publications/pdf/RS_No58/No58_10VE_Hilger1.pdf
What are the rules to be followed for the implementation of this tool?	The decision as to the permissibility of controlled transportation is taken by the responsible public prosecutor. He/she informs the public prosecutor from whose district the transportation is likely to leave domestic territory. The public prosecutor responsible for the place of importation is also to be informed if another than this one is operating the proceedings.	https://www.unafei.or.jp/publications/pdf/RS_No58/No58_10VE_Hilger1.pdf
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	One specific case in which controlled delivery is not implemented or must be aborted is when it comes to human trafficking.	https://www.unafei.or.jp/publications/pdf/RS_No58/No58_10VE_Hilger1.pdf
What authorisation is needed for the use of this tool?	see above	see above
What ongoing supervision is required for the use of this tool?	With controlled delivery the public prosecutor is on principle responsible for the proceedings of items related to the offence are brought onto domestic territory. This also applies to controlled	https://www.unafei.or.jp/publications/pdf/RS_No58/No58_10VE_Hilger1.pdf

Relevant items	Provisions	Sources used
	importation. With controlled exportation, the proceedings are on principle operated by the public prosecutor from whose district the transportation is initiated.	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Data available on the number of times this tool has been used for SOC cases	N/A	
Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	1) German police or prosecutors have to adhere to different rules of the respective state. There is no common framework. Since border security is one of the tasks of the Federal Police ("Bundespolizei"), it can be assumed that cross-border pursuits also fall within the remit of the Federal Police. The basis of the Federal Police is the Federal Police Act (2 - Bundespolizeigesetz) and Administrative Enforcement Act (3 - Verwaltungsvollstreckungsgesetz). 4) Schengen Convention (SDÜ) Article 41 5) In addition, there is a contract between Austria and Germany. According to the contract under Article 12, Article 41 of the Schengen Convention applies with certain additions for cross-border pursuit between Germany and Austria.	1) Overview: https://www.qdp.de/qdp/qdpnrw.nsf/id/953562AE7EFE0D9BC1257CDE00452C56/\$file/Polizeigesetze_Laender.pdf?open 2) Bundespolizeigesetz (BPolG): https://www.gesetze-im-internet.de/bqsg_1994/BJNR297900994.html 3) Verwaltungsvollstreckungsgesetz (VwVG) 4) Schengen Convention Article 41 (1): https://www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10006045&FassungVom=2017-09-25&Artikel=41&Paragraf=&Anlage=&Uebergangsrecht= 5) https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20004503
How is the tool defined?	1) According to the Schengen Convention in Article 41 (1), officers of a Contracting Party who are pursuing in their country a person caught in the act of committing or participating in an offense are authorised to continue the pursuit in the territory of another Contracting Party without the latter's prior consent if, due to the particular urgency of the matter, the competent authorities of the other Contracting Party could not be informed beforehand by one of the designated means of communication or are not on hand in time to take over the pursuit. 2) According to the contract between Austria and Germany, Article 41 of the Schengen Convention applies with certain additions (article 12 of the contract) for cross-border pursuit between Germany and Austria: - In addition to the purposes referred to in Article 41, paragraph 1, of the Schengen Convention, cross-border hot pursuit shall also be permitted, within the limits of the domestic law of the Contracting States in force, in the pursuit of persons who, within a distance of not more than 150 kilometres from the border, are evading control for the purpose of tracing persons suspected of having committed an extraditable offence or who have been sentenced to a custodial sentence in respect of which extradition appears to be permitted. Hot pursuit shall also take place across air and water borders. Entry into dwellings and properties not accessible to the public shall not be permitted. Publicly accessible work, operating and business premises may be entered during working, operating and business hours.	1) Schengen Convention Article 41 (1): https://www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10006045&FassungVom=2017-09-25&Artikel=41&Paragraf=&Anlage=&Uebergangsrecht= 2) https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20004503
For what types of crime can the tool be used?	According to article 41 of the Schengen Convention, the tool can be used for: - Murder, manslaughter, rape, Intentional arson, counterfeiting, Grand larceny, receiving stolen goods and robbery, extortion, kidnapping and hostage-taking, trafficking in human beings, illicit traffic in narcotics, Violation of legal regulations concerning weapons and explosives, Destruction by explosives, unauthorised circulation of toxic and harmful wastes, Unauthorised removal after an accident resulting in serious bodily injury or death	Schengen Convention Article 41 (1): https://www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10006045&FassungVom=2017-09-25&Artikel=41&Paragraf=&Anlage=&Uebergangsrecht=
Does national law allow this tool to be used in cross border cases?	Yes, national law allow this tool to be used in cross-border cases.	- Schengen Convention Article 41 (1): https://www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10006045&FassungVom=2017-09-25&Artikel=41&Paragraf=&Anlage=&Uebergangsrecht= https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20004503
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	According to Article 41 of the Schengen Convention, the pursuing officers must contact the competent authority of the territorial state at the latest when crossing the border.	Schengen Convention Article 41 (1): https://www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10006045&FassungVom=2017-09-25&Artikel=41&Paragraf=&Anlage=&Uebergangsrecht=
Which LEAs can use this tool?	According to Article 41 (7) of the Schengen Convention, the following officials of the Federal Republic of Germany are involved: The officers of the federal and state police forces and, limited to the area of illicit traffic in narcotics and illicit trafficking in weapons, the officers of the customs investigation service as auxiliary officers of the public prosecutor's office	Schengen Convention Article 41 (7): https://www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10006045&FassungVom=2017-09-25&Artikel=41&Paragraf=&Anlage=&Uebergangsrecht=
What are the rules to be followed for the implementation of this tool?	see above (column D25 & D21)	see above (column D25 & D21)

Relevant items	Provisions	Sources used
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	There is no special authorisation needed, but the pursuing officers must contact the competent authority of the territorial state at the latest when crossing the border.	Schengen Convention Article 41 (1): https://www.ris.bka.gv.at/NormDokument.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10006045&FassungVom=2017-09-25&Artikel=41&Paragraf=&Anlage=&Uebergangsrecht=
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	Zeugenschutz-Harmonisierungsgesetz (ZSHG) - in engl.: Witness Protection Harmonisation Act	ZSHG: http://www.gesetze-im-internet.de/zshg/__1.html
How is the tool defined?	According to Article 1 (1) of the ZSHG: A person without whose information in criminal proceedings the investigation of the facts or the determination of the whereabouts of the accused would be futile or substantially impeded may, with his or her consent, be protected in accordance with the provisions of this Act if, because of his or her willingness to testify, he or she is exposed to a risk to life, limb, health, freedom or substantial property and is suitable for witness protection measures.	ZSHG Article 1 (1): http://www.gesetze-im-internet.de/zshg/__1.html
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	According to § 5 ZSHG, the witness protection services are obliged to provide the persons to be protected with documents and evidence on the basis of which a fictitious curriculum vitae can be reconstructed (camouflage identity).	Article 5: http://www.gesetze-im-internet.de/zshg/__5.html
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	The consent of the public prosecutor's office shall be obtained for the commencement and termination of witness protection.	Article 2 (4) http://www.gesetze-im-internet.de/zshg/__2.html
What ongoing supervision is required for the use of this tool?	Since all measures taken in the context of witness protection, such as the issuance of cover papers, financial benefits, or the termination of witness protection, can be reviewed by administrative courts at any time, the witness protection services are obliged to keep complete documentation. A regulation on this can be found in Article 2 (3) ZSHG.	Article 2 (3) http://www.gesetze-im-internet.de/zshg/__2.html
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Surveillance		
Relevant documents (legal and non-legal) that define the functioning of the tool	1) The short-term observation is permitted under German law without further investigation as a general measure in the Code of Criminal Procedure (StPO) under §163. 2) §163f StPO: https://www.gesetze-im-internet.de/stpo/_163f.html	1) §163 StPO: https://www.gesetze-im-internet.de/stpo/_163.html 2) §163f StPO: https://www.gesetze-im-internet.de/stpo/_163f.html

Relevant items	Provisions	Sources used
	2) The focus of the following explanations is for long-term observations, which are regulated in the Code of Criminal Procedure (StPO) under §163f.	
Specific range of application of the tool	Further specific monitoring/Surveillance is regulated under: a) 100a StPO: Telecommunications surveillance Telecommunications may also be monitored and recorded without the knowledge of the persons concerned if: 1. if certain facts give rise to the suspicion that someone has committed a serious criminal offence as a perpetrator or participant, attempted to commit a serious criminal offence in cases where the attempt is punishable, or prepared to commit a criminal offence by committing a criminal offence 2. the offence is also serious in the individual case 3. if the investigation of the facts or the determination of the whereabouts of the accused would otherwise be significantly impeded or futile. b) 100c StPO: acoustic surveillance of living space Even without the knowledge of the persons concerned, the spoken word spoken in a dwelling in a non-public manner may be intercepted and recorded by technical means if: 1. certain facts give rise to the suspicion that someone has committed a particularly serious criminal offence specified in Section 100b (2) as a perpetrator or participant or has attempted to commit such an offence in cases where the attempt is punishable, 2. the offence is also particularly serious in the individual case, 3. on the basis of factual indications it can be assumed that the surveillance will record statements made by the accused which are of importance for the investigation of the facts of the case or for the determination of the whereabouts of a coaccused, and 4. the investigation of the facts or the determination of the whereabouts of a co-defendant would otherwise be disproportionately difficult or futile. b) 100f StPO: acoustic monitoring outside living space Even without the knowledge of the persons concerned, the non-public spoken word may be intercepted and recorded by technical means outside of homes if certain facts give rise to the suspicion that someone, as a perpetrator or participant, has committed or, in cases where the attempt is punishable, attempted to commit a serious criminal offense specified in Section 100a (2), even in individual cases, and the investigation of the facts or the determination of the whereabouts of an accused person would otherwise be futile or substantially impeded. [could you summarise the activities under each] JMA: done	• §100a StPO: https://www.gesetze-im-internet.de/stpo/_100a.html • §100c StPO: https://www.gesetze-im-internet.de/stpo/_100c.html • §100f StPO: https://www.gesetze-im-internet.de/stpo/_100f.html
How is the tool defined?	Long-term observations are defined as observations of defendants that 1. consistently last longer than 24 hours or occur on more than two days.	• §163f StPO: https://www.gesetze-im-internet.de/stpo/_163f.html
For what types of crime can the tool be used?	There is no description or restriction for which types of crimes a long-term observation can be used.	• §163f StPO: https://www.gesetze-im-internet.de/stpo/_163f.html
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	The measure may only be ordered if the investigation of the facts or the determination of the whereabouts of the perpetrator would be considerably less promising or considerably more difficult by other means. The measure is permissible against other persons if it can be assumed on the basis of certain facts that they are connected with the perpetrator or such a connection is established that the measure will lead to the investigation of the facts or the determination of the whereabouts of the perpetrator and this would be considerably less promising or considerably more difficult in another way. [this is useful. was there nothing at all on the types (or seriousness) of the crime?] JMA: No, there was no further information about the types or seriousness of the crime	• §163f StPO: https://www.gesetze-im-internet.de/stpo/_163f.html
What types of stakeholder are involved in the implementation of this tool?	The measure may be ordered only by the court, and in case of imminent danger also by the public prosecutor's office and its investigators.	• §163f StPO: https://www.gesetze-im-internet.de/stpo/_163f.html
Which LEAs can use this tool?	1) According to the Federal Police Act (BPolG), the Federal Police (Bundespolizei) may conduct long-term observations. 2) According to the Federal Criminal Police Act (BKAG), the Federal Criminal Police Office (Bundeskriminalamt) is allowed to conduct long-term observations to defend against international terrorism.	• 1) §28 BPolG: https://www.gesetze-im-internet.de/bpgsg_1994/_28.html • 2) §45 BKAG: https://www.gesetze-im-internet.de/bkag_2018/_45.html
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	The measure may be ordered only by the court, and in case of imminent danger also by the public prosecutor's office and its investigators. The order of the public prosecutor's office or its	• §163f StPO: https://www.gesetze-im-internet.de/stpo/_163f.html

Relevant items	Provisions	Sources used
	investigators shall cease to have effect if it is not confirmed by the court within three working days.	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Undercover / covert operations		
Relevant documents (legal and non-legal) that define the functioning of the tool	Under §110a of the Code of Criminal Procedure (StPO), the prerequisites for the use of undercover investigators and under §110c, the powers of an undercover investigator are stipulated.	1) § 110a StPO: https://www.gesetze-im-internet.de/stpo/_110a.html 2) §110c StPO: https://www.gesetze-im-internet.de/stpo/_110c.html
How is the tool defined?	Undercover investigators are officers of the police service who investigate under a changed identity (legend) that has been given to them and is intended to be permanent. They are allowed to participate in legal transactions under this legend (§101 (2) StPO). §110a (3) StPO: Insofar as it is indispensable for the construction or maintenance of the legend, corresponding documents may be produced, altered and used.	§101 (2) StPO: https://www.gesetze-im-internet.de/stpo/_101.html § 110a StPO: https://www.gesetze-im-internet.de/stpo/_110a.html
For what types of crime can the tool be used?	Undercover investigators may be used to investigate criminal offences if there are sufficient factual indications that a criminal offence of considerable importance has been committed 1. in the field of illicit narcotics or weapons trafficking, counterfeiting of currency or stamps, 2. in the field of state protection, 3. on a professional or habitual basis, or 4. committed by a gang member or otherwise organised.	§ 110a StPO: https://www.gesetze-im-internet.de/stpo/_110a.html
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	Decisions and other documents concerning measures pursuant to, inter alia, Section 110a shall be kept by the Public Prosecutor's Office	§101 (2) StPO: https://www.gesetze-im-internet.de/stpo/_101.html
Which LEAs can use this tool?	§ 110a (2): Undercover investigators are officers of the police service who investigate under a changed identity (see above).	§ 110a (2) StPO: https://www.gesetze-im-internet.de/stpo/_110a.html
What are the rules to be followed for the implementation of this tool?	The use of undercover agents is only permissible if the investigation would otherwise be futile or considerably more difficult. Undercover agents may also be used to solve crimes if the special significance of the crime requires their use and other measures would be futile.	§110a StPO: https://www.gesetze-im-internet.de/stpo/_110a.html
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	I) §110b (1): The use of an undercover investigator shall only be permitted after the public prosecutor's office has given its consent. If there is imminent danger and the decision of the public prosecutor's office cannot be obtained in time, it shall be obtained without delay; the measure shall be terminated unless the public prosecutor's office consents within three working days. The consent shall be given in writing and shall be limited in time. An extension is permissible as long as the prerequisites for the assignment continue to exist. II) §110b (2): Operations directed against a specific defendant or in which the undercover agent enters a dwelling that is not generally accessible require court approval.	§110b StPO: https://www.gesetze-im-internet.de/stpo/_110b.html
What ongoing supervision is required for the use of this tool?	The use of undercover investigators and other police officers who are not openly investigating shall be documented. The documents, unless they are to be included in the investigation files, are to be kept locked for the use of undercover investigators according to more detailed instructions of the director of the State Criminal Police Office, and for the use of other police officers who are not openly investigating, according to more detailed instructions of the management of the competent police authority and are to be kept secret.	https://recht.nrw.de/lmi/owa/br_bes_text?anw_nr=1&gld_nr=2&uql_nr=2056&bes_id=3254&val=3254&ver=7&sq=&aufgehoben=N&menu=1
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime	N/A	

Relevant items	Provisions	Sources used
cases? If yes can you please indicate the relevant statistics?		
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	Police law in Germany depends on the respective federal state. Exemplary for the police law of North Rhine-Westphalia: §19 PolG NRW - Data collection through the use of persons whose cooperation with the police is not known to third parties.	§19 PolG NRW: http://www.lexsoft.de/cgi-bin/lexsoft/justizportal_nrw.cgi?t=148302810403357818&xid=167231,22
Specific range of application of the tool	A distinction must be made between 1) informants and 2) V-persons: 1) Informants are not V-persons, but private individuals who are prepared in individual cases to provide information to the law enforcement agency in return for an assurance of confidentiality. These are persons who have contacts in a field of observation and who are willing to provide the police with relevant information if necessary. Such persons are not "controlled" by the police in a targeted manner. 2) V-persons help the police in their investigative work without being members of the authority themselves. They are, so to speak, "freelance" employees who have access to the persons, associations or organisations about which information is needed from the police point of view in order to fulfil police tasks. V-persons are paid for their activities.	https://www.rodorf.de/01_polg/19polg.htm#VVPolG
How is the tool defined?	see above	see above
For what types of crime can the tool be used?	There is no description or restriction for which types of crime the tool can be used.	https://recht.nrw.de/lmi/owa/br_bes_text?anw_nr=1&qld_nr=2&uql_nr=2056&bes_id=3254&val=3254&ver=7&sq=&aufgehoben=N&menu=1
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	1) Informants: The following shall decide on the assurance of confidentiality: a) in the business area of the police headquarters, the management of the Directorate of Crime, b) in the business area of the district councils as district police authorities, the management of the department of the police c) in the business area of the State Office of Criminal Investigation, the management of the competent department. In case of imminent danger, the next superiors shall decide. 2) V-persons: The following shall decide on the assurance of secrecy: a) in the business area of the police headquarters, the management of the Directorate of Crime, b) in the business area of the district councils as district police authorities, the management of the department of the police c) in the business area of the State Criminal Police Office, the management of the competent department. Prior to the targeted use of confidential informants the consent of the person entitled to the assurance of secrecy in the police authority conducting the investigation must be obtained. [though interesting, this is not an answer to the question] JMA: Depending on whether Informants or V-Persons, it lists who makes the decision, such as Police headquarters. If that does not answer the question, please specify.	https://recht.nrw.de/lmi/owa/br_bes_text?anw_nr=1&qld_nr=2&uql_nr=2056&bes_id=3254&val=3254&ver=7&sq=&aufgehoben=N&menu=1
Which LEAs can use this tool?	Federal police, state police and prosecutors office can use informants.	https://recht.nrw.de/lmi/owa/br_bes_text?anw_nr=1&qld_nr=2&uql_nr=2056&bes_id=3254&val=3254&ver=7&sq=&aufgehoben=N&menu=1
What are the rules to be followed for the implementation of this tool?	The use of informants and the use of V-Persons require a balancing of the criminal procedural requirements of the immediacy of the taking of evidence and the complete investigation of the facts on the one hand, and the fulfilment of public duties through the assurance of confidentiality/secrecy on the other. In this context, the principle of a fair trial under the rule of law must be observed. Informants may only be assured of confidentiality if their cooperation with the law enforcement authorities would be significantly endangered or they would have to expect unreasonable disadvantages if it became known.	https://recht.nrw.de/lmi/owa/br_bes_text?anw_nr=1&qld_nr=2&uql_nr=2056&bes_id=3254&val=3254&ver=7&sq=&aufgehoben=N&menu=1
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	The use of minors as V-persons is not permitted.	https://recht.nrw.de/lmi/owa/br_bes_text?anw_nr=1&qld_nr=2&uql_nr=2056&bes_id=3254&val=3254&ver=7&sq=&aufgehoben=N&menu=1
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	§19 (2) PolG NRW: The deployment of persons whose cooperation with the police is not known to third parties may only be ordered by the head of the authority or a senior police enforcement service manager appointed by them.	§19 PolG NRW: http://www.lexsoft.de/cgi-bin/lexsoft/justizportal_nrw.cgi?t=148302810403357818&xid=167231,22
What ongoing supervision is required for the use of this tool?	The use of informants and the cooperation of the police with informants shall be documented. The documents, unless they are to be included in the investigation files, are to be kept locked up and kept secret in accordance with more detailed instructions from the management of the police authority.	https://recht.nrw.de/lmi/owa/br_bes_text?anw_nr=1&qld_nr=2&uql_nr=2056&bes_id=3254&val=3254&ver=7&sq=&aufgehoben=N&menu=1
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	

Relevant items	Provisions	Sources used
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	

Source: Author's own elaboration

Greece

Table 29 – Overview of national rules on investigative tools - Greece

Relevant items	Provisions	Sources used
Controlled Delivery		
Relevant documents (legal and non-legal) that define the functioning of the tool	Law 2145/93 Law 2331/95	- Law - 2145/1993 - Government Gazette 88/A/28-5-1993 - Regulation of matters related to execution of punishments and streamline procedures administration of justice and other issues - Law - 2331/1993 - Government Gazette 173/A/24-8-1995 - "Prevention and combating of the legalisation of income from criminal activities" and other penal rules - Full member meetings of the Supreme Court (Arios Pagos) - Arbitrations and other provision's
How is the tool defined?	There is no specific definition in Greek Laws	https://www.unodc.org/pdf/convention_1988_en.pdf
For what types of crime can the tool be used?	Drugs	- Law 2145/93 - - Article 38 of Law 2145/93 - Paragraph 2 Article 38 of Law 2145/93
Does national law allow this tool to be used in cross border cases?	The Appeals Prosecutor of Athens, where the guarantees provided by the requesting State ensure the control of shipment and the arrest of persons involved in the case, notify the Prosecutors who must, post the above notice, to refrain from prosecution and to act as what is necessary in order not to interrupt the transfer	
What thresholds must be passed for the use of this tool?	According to the article 11 of the Vienna Convention of 1988 (N.1990/91) of the United Nations, the requests of the Member aliens, are subjected to any kind of transmission, but still writing, directly or through Interpol to the Coordinating Unit Against Drug Trafficking, which, after checking the legal origin and the legality of the request, shall immediately report to the Appeals Prosecutor of Athens in a confidential letter, to which he attaches a copy of the telegram or any other document containing the application	Paragraph 1 Article 15 of Law 2331/95
What types of stakeholder are involved in the implementation of this tool?	The Appeals Prosecutor of Athens notify the Prosecutors who must refrain from prosecution and to act as what is necessary in order not to interrupt the transfer. The Coordinating Unit Against Drug Trafficking has the authority and responsibility of the transport throughout from the entrance to the exit of the drugs from the country	Law 2145/93
Which LEAs can use this tool?	Coordinating Unit Against Drug Trafficking: Hellenic Police, Customs, Coast Guard and Financial and Economic Crime Unit	http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=2676&Itemid=0&lang=
What are the rules to be followed for the implementation of this tool?	- According to the article 11 of the Vienna Convention of 1988 (N.1990/91) of the United Nations, the requests of the Member aliens, are subjected to any kind of transmission, but still writing, directly or through Interpol to the Coordinating Unit Against Drug Trafficking, which, after checking the legal origin and the legality of the request, shall immediately report to the Appeals Prosecutor of Athens in a confidential letter, to which he attaches a copy of the telegram or any other document containing the application. - The Appeals Prosecutor of Athens, where the guarantees provided by the requesting State ensure the control of shipment and the arrest of persons involved in the case, notify the Prosecutors who must, post the above notice, to refrain from prosecution and to act as what is necessary in order not to interrupt the transfer. - The Coordinating Unit Against Drug Trafficking has the authority and responsibility of the transport throughout from the entrance to the exit of the drugs from the country. - Immediately after the removal of drugs from the country and at the latest within 48 hours, the above service issues a report stating in detail all about the performed under the control of transport, and in particular the date, time and place of entry and exit drugs from the country. A copy of the report shall be submitted to confidential document to the Appeals Prosecutor of Athens. - Domestic judicial authority's requests to conduct controlled delivery outside the Greek territory are transmitted through the Appeals Prosecutor of Athens to the Coordinating Unit Against Drug Trafficking. Settings of the previous paragraph also apply in this case.	- Paragraph 1 Article 15 of Law 2331/95 - Article 38 of Law 2145/93
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	

Relevant items	Provisions	Sources used
What authorisation is needed for the use of this tool?	The Appeals Prosecutor of Athens notify the Prosecutors who must refrain from prosecution and to act as what is necessary in order not to interrupt the transfer.	Law 2145/93
What ongoing supervision is required for the use of this tool?	Immediately after the removal of drugs from the country and at the latest within 48 hours, the above service issues a report stating in detail all about the performed under the control of transport, and in particular the date, time and place of entry and exit drugs from the country. A copy of the report shall be submitted to confidential document to the Appeals Prosecutor of Athens	Law 2145/93
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Data available on the number of times this tool has been used for SOC cases	N/A	
Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	Article 41 of Law 2514/1997	Law 2514/1997 - Government Gazette 140/A/27-6-1997 -Implementing the Schengen Agreement
How is the tool defined?	Officers of one of the Contracting Parties who are pursuing in their country an individual caught in the act of committing or of participating in one of the offences referred to in paragraph 4 shall be authorised to continue pursuit in the territory of another Contracting Party without the latter's prior authorisation where, given the particular urgency of the situation, it is not possible to notify the competent authorities of the other Contracting Party by one of the means provided for in Article 44 prior to entry into that territory or where these authorities are unable to reach the scene in time to take over the pursuit. Paragraph 4 Article 41 of Law 2514/1997 the Contracting Parties shall define the offences referred to in paragraph 1 in accordance with one of the following procedures: (a) The following criminal offences: murder, manslaughter, rape, arson, forgery of money, aggravated burglary and robbery and receiving stolen goods, extortion, kidnapping and hostage taking, trafficking in human beings, illicit trafficking in narcotic drugs and psychotropic substances, breach of the laws on arms and explosives, wilful damage through the use of explosives, illicit transportation of toxic and hazardous waste, failure to stop and give particulars after an accident which has resulted in death or serious injury. (b) Extraditable offences.	Paragraph 1 & Paragraph 4, Article 41 of Law 2514/1997
For what types of crime can the tool be used?	Cross crime areas	Paragraph 4, Article 41 of Law 2514/1997
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	It is not clearly clarified. The LEAs that are allowed to use the tool are the pursuing officers of Greece.	Article 41 of Law 2514/1997
What are the rules to be followed for the implementation of this tool?	Hot pursuit shall be carried out only under the following general conditions: (a) The pursuing officers must comply with the provisions of this Article and with the law of the Contracting Party in whose territory they are operating; they must obey the instructions issued by the competent local authorities. (b) Pursuit shall be solely over land borders. (c) Entry into private homes and places not accessible to the public shall be prohibited. (d) The pursuing officers shall be easily identifiable, either by their uniform, by means of an armband or by accessories fitted to their vehicles; the use of civilian clothes combined with the use of unmarked vehicles without the aforementioned identification is prohibited; the pursuing officers must at all times be able to prove that they are acting in an official capacity. (e) The pursuing officers may carry their service weapons; their use shall be prohibited save in cases of legitimate self-defence. (f) Once the pursued person has been apprehended as provided for in paragraph 2(b), for the purpose of being brought before the competent local authorities that person may only be subjected to a security search; handcuffs may be used during the transfer; objects carried by the pursued person may be seized. (g) After each operation referred to in paragraphs 1, 2 and 3, the pursuing officers shall appear before the competent local authorities of the Contracting Party in whose territory they were operating and shall report on their mission; at the request of those authorities, they shall remain at their disposal until the circumstances surrounding their action have been sufficiently clarified;	Paragraph 5, Article 41 of Law 2514/1997

Relevant items	Provisions	Sources used
	this condition shall apply even where the hot pursuit has not resulted in the arrest of the person pursued. (h) The authorities of the Contracting Party from which the pursuing officers have come shall, when requested by the authorities of the Contracting Party in whose territory the hot pursuit took place, assist the enquiry subsequent to the operation in which they took part, including judicial proceedings.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Police officers from Greece authorized to continue pursuit in the territory of another Contracting Party Contracting of Schengen Convention Police officers from Greece authorised to continue pursuit in the territory of another Contracting Party Contracting of Schengen Convention Bordering countries of Greece are Turkey, Albania, FYROM and Bulgaria. However these countries have not joined the Schengen Area.	Article 41 of Law 2514/1997
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	Article 9 & 10 Law 2928/2001	Law - 2928/2001 - Government Gazette 141/A/27-6-2001 - Amendment of provisions of the Criminal Code and of the Code of Criminal Procedure and other provisions on citizens' protection from offences of criminal organisations
How is the tool defined?	Article 9 Law 2928/2001 Law 2928/2001 on the protection of citizens against criminal acts by organised crime and terrorist groups. Article 9 of the above law states that during the prosecution of these crimes all measures may be taken in order to effectively protect the main witnesses, or their relatives, from possible revenge actions or intimidation.	Paragraph 1, Article 9 of Law 2928/2001
For what types of crime can the tool be used?	Cross crime areas	Article 9 Law 2928/2001
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	Public Prosecutor - Recommendation for witness protection Hellenic Police - witness protection	Article 9 Law 2928/2001
Which LEAs can use this tool?	Hellenic Police	Article 9 Law 2928/2001
What are the rules to be followed for the implementation of this tool?	The special protective regime is only granted with the consent of the person concerned and the specific measures taken must not limit their personal freedom unduly and beyond what is strictly necessary under the circumstances of the case. Protective measures may be removed when the protected person requests in writing or when they do not cooperate effectively with the authorities.	Paragraph 2, Article 9 Law 2928/2001
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime	N/A	

Relevant items	Provisions	Sources used
cases? If yes can you please indicate the relevant statistics?		
Surveillance		
Relevant documents (legal and non-legal) that define the functioning of the tool	Law 4620/2019	• Law 4620/2019 Government Gazette 96/A/11-6-2019 - New Criminal Procedure Code
Specific range of application of the tool	In National Legislation there are not mentioned the types of surveillance activities	• Article 251 of Law 4620/2019
How is the tool defined?	There is no specific definition in the law	•
For what types of crime can the tool be used?	Cross crime areas • According to article 251 of New Criminal Procedure Code, the persons who are ordered by the Public Prosecutor to conduct investigation must collect evidence and information by using in general any legal means necessary. • According to "Study on paving the way for future policy initiatives in the field of fight against organised crime: the effectiveness of specific criminal law measures targeting organised crime", in Greece surveillance is carried out by personnel of the State Security Division of Hellenic Police and by subdivisions investigating organised crime, drug trafficking, and economic crime.	• 1. Article 251 of Law 4620/2019 • 2. "Study on paving the way for future policy initiatives in the field of fight against organised crime: the effectiveness of specific criminal law measures targeting organised crime" of European Commission: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/20150312_1_amoc_report_020315_0_220_part_2_en.pdf
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	Judicial authority – prosecutors; Hellenic Police	• Article 251 of Law 4620/2019
Which LEAs can use this tool?	Hellenic Police	• Article 251 of Law 4620/2020
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Undercover / covert operations		
Relevant documents (legal and non-legal) that define the functioning of the tool	• Law 2713/1999 Government Gazette 89/A/30-4-1999 - Initiation of the Division of Internal Affairs of the Hellenic Police • Law 2161/1993 Government Gazette 119/A/26-7-1993 - Combating the spread of drugs, protection of young people and other provisions • Law 2648/1998 Government Gazette 238/A/22-10-1998 - Amendment of the Code of Tax Procedure and other provisions. • Law 3028/2002 Government Gazette 153/A/28-06-2002 - Protection of Antiquities and Cultural Heritage in general	• Article 5 of Law 2713/99 • Article 22 of Law 2161/93 • Article 33 of Law 2648/98 • Article 68 of Law 3028/02
How is the tool defined?	It isn't inequitable the act of a policeman, a custom officer, an employee of the Financial and Economic Crime Unit and a port personnel, who, with the command of the competent for prosecuting drug trafficking head and in order to discover or arrest a person, committing a crime than those mentioned in Articles 5 and 8 of Law 1729/87, appears as a prospective buyer or carrier or generally interested in the handling, storage or disposal of drugs. Article 5 & 8 of 1729/87 - Drug related crimes	• Article 22 of Law 2161/93
For what types of crime can the tool be used?	cross crime areas	• 1. Article 5 of Law 2713/99 • 2. Article 22 of Law 2161/93 • 3. Article 33 of Law 2648/98 • 4. Article 68 of Law 3028/02

Relevant items	Provisions	Sources used
	- Article 5 of Law 2713/99 - A policeman of the Internal Affairs Service when, ordered by the Chief and with the purpose of discovery or arrest a person involved in crime, appears as a participant of the act - Article 22 of Law 2161/93 & Article 33 of Law 2648/98 - A policeman, a custom officer, an employee of the Financial and Economic Crime Unit and a port personnel, who, with the command of the competent for prosecuting drug trafficking head and in order to discover or arrest a person, committing a crime. - Article 68 of Law 3028/02 - Covert operations are applied accordingly to the crimes of theft monuments, monuments of misappropriation, deterioration of monuments, acceptance and disposal of monuments that are the proceeds of crime, illegal excavations or other archaeological research and the illicit export of cultural goods	
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	Hellenic police Custom officer Employee of the Financial and Economic Crime Unit Port personnel	Article 22 of Law 2161/93
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	Article 187C of Law 4619/2019	Law 4619/2019 Government Gazette 95/A/11-6-2019 - New Penal Code
Specific range of application of the tool	- Member of an Organised Criminal Group (OCG) - Members in terrorist organisations	Article 187C of Law 4619/2019
How is the tool defined?	A person guilty of the acts of forming or joining a criminal organisation or conspiracy within the meaning of Article 187(1) and (3) or of forming or joining a terrorist gang within the meaning of Article 187A who reports and thus makes it possible to prevent the commission of a planned crime or thus materially helps to dismantle the criminal organisation or conspiracy or terrorist gang shall be exempt from punishment for those acts. If no criminal proceedings have yet been initiated, the public prosecutor of the lower criminal courts shall issue a reasoned order preventing criminal proceedings from being initiated and shall forward the case file to the public prosecutor to the appeal courts, who shall act in accordance with Article 43(2) of the Code of Penal Procedure.	Article 187C of Law 4619/2019
For what types of crime can the tool be used?	Cross crime areas Article 187C of Law 4619/2019 A person guilty of the acts of forming or joining a criminal organisation or conspiracy who reports and thus makes it possible to prevent the commission of a planned crime or thus materially helps	Article 187C of Law 4619/2019

Relevant items	Provisions	Sources used
	to dismantle the criminal organisation or conspiracy or terrorist gang shall be exempt from punishment for those acts.	
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	Judicial authority	Article 187C of Law 4619/2019
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	

Source: Author’s own elaboration

Hungary

Table 30 – Overview of national rules on investigative tools - Hungary

Relevant items	Provisions	Sources used
Controlled Delivery		
Relevant documents (legal and non-legal) that define the functioning of the tool	- Act XC of 2017 on criminal proceedings, CHAPTER XXXVIII. Secret surveillance authorised by the judge, Section 231 (1) d) - Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I, General Provision, Article 15	- Act XC of 2017 on criminal proceedings, CHAPTER XXXVIII. Secret surveillance authorised by the judge, Section 231 (1) d) - Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I, General Provision, Article 15
How is the tool defined?	- Controlled Delivery: Upon Letter of Request from a Contracting Party, another Contracting Party can, in case of investigations for extraditable offences, if appropriate, permit controlled delivery on its territory, especially of transport of narcotic drugs, precursors, firearms, explosives, counterfeit currency, and items originating from a crime, or intended to be used to commit a crime. The requested Contracting Party shall take control over the delivery when it crosses the border, or at a place of taking over agreed by the law enforcement authorities, in order to avoid interruption of control, and guarantees permanent surveillance of the shipment in a manner that enables police intervention at any time. After takeover by the requested Contracting Party, officers of the requesting Contracting Party can continue to follow the controlled delivery together with officers of the requested Contracting Party, upon agreement with the requested Contracting Party. - Secret knowledge of a shipment: secret knowledge of a shipment (open mail or other sealed mail in secret, get to know its contents, check it and record it	- Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I, General Provision, Article 15 (1), (2) - Act XC of 2017 on criminal proceedings, CHAPTER XXXVIII. Secret surveillance authorised by the judge, Section 231 (1) d)
For what types of crime can the tool be used?	- Transport of narcotic drugs, precursors, firearms, explosives, counterfeit currency, and items originating from a crime, or intended to be used to commit a crime. - Secret knowledge of a shipment: cross crime areas	- Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I, General Provision, Article 15 (1) - Act XC of 2017 on criminal proceedings, CHAPTER XXXVIII. Secret surveillance authorised by the judge, Section 231 (1) d)
Does national law allow this tool to be used in cross border cases?	Controlled delivery regulated in Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I, General Provision, Article 15: can be used for cross border criminal investigations. However it can be also used for cross border criminal investigations as defined in the Act XC of 2017 on criminal proceedings and in the Act CLXXX of 2012 on criminal cooperation with the Member States of the European Union.	- Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I, General Provision, Article 15 (1) - Act CLXXX of 2012 on criminal cooperation with the Member States of the European Union Section 2 and Section 59/A g); Section 69/E-69/H

Relevant items	Provisions	Sources used
	Secret knowledge of a shipment: can be used for national criminal investigation	Act XC of 2017 on criminal proceedings, CHAPTER XXXVIII. Secret surveillance authorised by the judge, Section 231 (1) d)
What thresholds must be passed for the use of this tool?	- Secret knowledge of a shipment is a covert operation which must be authorised by the judge (in exceptional cases by the prosecutor). This covert operation can be only used for intentional offences punishable by a custodial sentence of up to five years or more, or intentional offences determined in Section 234 (2) and punishable by a custodial sentence of up to 3 years or more such as child prostitution, child pornography, corruption offences, offences against referendum and EU citizens' initiative, sexual abuse, drug precursor abuse. - The requesting Contracting Party explains that, without such a measure, identification of perpetrators or of distributing routes would be impossible or extremely hampered. If the content of a controlled delivery presents a particular risk for the persons involved, or a danger to the public, the requested Contracting Party has the right to ask that certain conditions to be met before granting the request or refuse the request altogether.	- Act XC of 2017 on criminal proceedings, CHAPTER XXXVIII. Secret surveillance authorised by the judge, Section 231 (1) d) + Section 234 (1)-(2) - Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I, General Provision, Article 15 (1)
What types of stakeholder are involved in the implementation of this tool?	It can be used by an authority which has the authorisation by the judge. According to Section 238 if the authorisation by the judge would cause such a delay that would significantly jeopardise the purpose, it can be authorised by the prosecutor. In this case the prosecutor can order the covert operations for 120 hours or until the judge's decision has been made.	Act XC of 2017 on criminal proceedings, CHAPTER XXXVIII. Secret surveillance authorised by the judge, Section 308 (1) on 231 (1) d) + Section 235-238
Which LEAs can use this tool?	- It can be used by an authority which has the authorisation by the judge. According to Section 238 if the authorisation by the judge would cause such a delay that would significantly jeopardise the purpose, it can be authorised by the prosecutor. In this case the prosecutor can order the covert operations for 120 hours or until the judge's decision. - The concealed operations can be used by the prosecutor, the police, the national security services and the National Tax and Customs Administration.	- Act XC of 2017 on criminal proceedings, CHAPTER XXXVIII. Secret surveillance authorised by the judge, Section 308 (1) on 231 (1) d) + Section 235-238 - Act XC of 2017 on criminal proceedings, CHAPTER L. Seizure, Section 309 (1)
What are the rules to be followed for the implementation of this tool?	- The main rule can be found in CHAPTER XXXVIII. Section 231. and Section 232 (4) and Section 233-234. However, there are certain rules which must be followed by the authorities performing a covert operation. These are the following: - Covert operation authorisation (Section 235-239); - Duration and extension of application (Section 239-243) - Withdraw and prohibit the covert operation (Section 242) - Implementation of covert operation (Section 243-245) - Termination of covert operation (Section 245) - Rules on data obtained in the use of covert operation (CHAPTER XL) - Results of the use of covert operation (CHAPTER XLI) - The officers of the requesting Contracting Party are obliged to observe the laws of the requested Contracting Party. Further rules are included in Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I, General Provision, Article 15 (2), (4)-(9)	- Act XC of 2017 on criminal proceedings, CHAPTER XXXVIII. Section 231. and Section 232 (4). - Covert operation authorisation (Section 235-239); - Duration and extension of application (Section 239-243) - Withdraw and prohibit the covert operation (Section 242) - Implementation of covert operation (Section 243-245) - Termination of covert operation (Section 245) - Rules on data obtained in the use of covert operation (CHAPTER XL) - Results of the use of covert operation (CHAPTER XLI) - Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I, General Provision, Article 15 (2)-(9)
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	- Secret knowledge of a shipment: The rules on Withdraw and prohibit the "secret knowledge of a shipment" operation can be found in the Act XC of 2017 on criminal proceedings Section 242. This Section regulates the cases when the judge can withdraw the authorisation (such as: the scope of the authorisation has been exceeded, the body authorised to use concealed means does not present the data within the time limit laid down in paragraph (1)). All the cases can be found in Section 242. Other relevant restrictions on data obtained in the use of covert operations can be found in CHAPTER XL. Furthermore other relevant rules on the implementation and termination of covert operations can be found in in Section 243-246. - Controlled Delivery: According to the Act XCII of 2012 on police cooperation convention for Southeast Europe Article 15 "If the person is not a national of the Contracting Party in whose territory he/she was arrested, that person shall be released no later than six hours after the arrest was made, not including the hours between midnight and 9.00 a.m., unless the competent local authorities have previously received a request for that person's provisional arrest for the purposes of extradition in any form whatsoever."	- Act XC of 2017 on criminal proceedings Section 242, 243-246 and CHAPTER XL. - Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I, General Provision, Article 15 (7)
What authorisation is needed for the use of this tool?	It can be used by an authority which has the authorisation by the judge. According to Section 238, if the authorisation by the judge would cause such a delay that would significantly jeopardise the aim, it can be authorised by the prosecutor. In this case the prosecutor can order the covert operations for 120 hours or until the judge's decision.	Act XC of 2017 on criminal proceedings, CHAPTER XXXVIII. Secret surveillance authorised by the judge, Section 231 (1) d) + Section 235-238
What ongoing supervision is required for the use of this tool?	According to Act XC of 2017 on criminal proceedings and Act XCII of 2012 on police cooperation convention for Southeast Europe, no supervisions required after the authorisation while the tool is being used.	Act XC of 2017 on criminal proceedings and Act XCII of 2012 on police cooperation convention for Southeast Europe
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	

Relevant items	Provisions	Sources used
Data available on the number of times this tool has been used for SOC cases	N/A	
Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	- Act LIV of 2002 on the international cooperation of the LEAs, CHAPTER III. Certain forms of cooperation, Section 31-33. - Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I. General provision, Article 13 + Article 24 Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER III. Final Provisions, Article 34	- Act LIV of 2002 on the international cooperation of the LEAs, CHAPTER III. Certain forms of cooperation, Section 31-33. - Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I. General provision, Article 13 + Article 24 - Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER III. Final Provisions, Article 34
How is the tool defined?	Hot Pursuit: Officers of one of the Contracting Parties who are pursuing in their country an individual caught in the act of committing or participating in a criminal offence shall be allowed, subject to bilateral Implementation Agreements concluded in accordance with Article 34 paragraph 1 of this Convention, to continue pursuit in the territory of another Contracting Party without the latter's prior authorisation, where given the particular urgency of the situation, it is not possible to notify the law enforcement authorities of the other Contracting Party by one of the means provided for in Article 24 of the Convention prior to entry into that territory or where these authorities are unable to reach the scene in time to take over the pursuit.	- Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I. General provision, Article 13 (1) +Article 24 - Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER III. Final Provisions, Article 34 (1)
For what types of crime can the tool be used?	It depends on the bilateral Implementation Agreements concluded in accordance with Article 34 paragraph 1 of this Convention, between the Contracting Parties.	- Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I. General provision, Article 13 (1) - Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER III. Final Provisions, Article 34 (1)
Does national law allow this tool to be used in cross border cases?	Hot Pursuit regulated in Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER III. Final Provisions, Article 13 can be used for cross border criminal investigations	Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I. General provision, Article 13 (1)
What thresholds must be passed for the use of this tool?	The bilateral Implementation agreements as referred to in paragraph 1 of this Article shall define the criminal offences for which the hot pursuit will be applicable either by way of an exhaustive list or by extending it to all extraditable criminal offences. The Act does not regulate the maximum term of imprisonment of crimes for which the tool can be used.	Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I. General provision, Article 13 (2)
What types of stakeholder are involved in the implementation of this tool?	Law enforcement authorities of the two contracting parties, which include pursuing an individual caught in the act of committing or participating in a criminal offence and the local authorities.	Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I. General provision, Article 13
Which LEAs can use this tool?	Police officers pursuing an individual caught in the act of committing or participating in a criminal offence.	Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I. General provision, Article 13
What are the rules to be followed for the implementation of this tool?	The main rules can be found in Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I. General provision, Article 13 (5): Hot pursuit shall be carried out only under the following general conditions: a) The pursuing officers must comply with the provisions of this Article and with the law of the Contracting Party in whose territory they are operating; they must follow the instructions issued by the competent local authorities. b) Pursuit shall be solely over land and blue borders. c) Entry into private homes and places not accessible to the public is prohibited. d) The pursuing officers shall be easily recognisable, either by their uniform, by means of an armband or by accessories fitted to their vehicles; the use of civilian clothes combined with the use of unmarked vehicles without the aforementioned identification is prohibited; the pursuing officers must at all times be able to prove that they are acting in an official capacity. e) The pursuing officers may carry their service weapons; their use shall be prohibited except in cases of legitimate self-defence. f) Once the pursued person has been apprehended as provided for in paragraph 3(b), for the purpose of being brought before the competent local authorities that person may only be subjected to a security search; handcuffs may be used during the transfer; objects carried by the pursued person may be seized. g) After each operation referred to in paragraphs 1, 3 and 4, the pursuing officers shall appear before the competent local authorities of the Contracting Party in whose territory they were operating and shall report on their mission; at the request of those authorities, they shall remain at their disposal until the circumstances surrounding their action have been sufficiently clarified; this condition shall apply even where the hot pursuit has not resulted in the arrest of the person pursued. h) The authorities of the Contracting Party from which the pursuing officers have come shall, when requested by the authorities of the Contracting Party in whose territory the hot pursuit took place, shall assist the enquiry subsequent to the operation in which they took part, including judicial proceedings, providing that the identity of the involved pursuing officer is protected. Other rules that apply to hot pursuit can be found in the Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I. General provision, Article 13 (3),(4), (6)	Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I. General provision, Article 13 (3)-(6)
Safeguards provided by national criminal laws to protect the rights of the	Some of the restrictions can be found in Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I. General provision, Article 13 (5), as mentioned above. Other	Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I. General provision, Article 13 (5)-(6)

Relevant items	Provisions	Sources used
individuals, ensure proportionality, and protect rule of law (if any)	restrictions to the use of the tool: A person who, following the action provided for in paragraph 3, has been arrested by the competent local authorities may, whatever that person's citizenship, be held for questioning. The relevant rules of national law shall apply mutatis mutandis. If the person is not a national of the Contracting Party in whose territory the person was arrested, that person shall be released no later than six hours after the arrest was made, not including the hours between midnight and 9.00 a.m., unless the competent local authorities have previously received a request for that person's provisional arrest for the purposes of extradition in any form whatsoever.	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	The bilateral Implementation agreements, which is agreed by the two Contracting Parties. The pursuing officers must comply with the provisions of this Article and with the law of the Contracting Party in whose territory they are operating; they must obey the instructions issued by the competent local authorities. The hot pursuit will cease as soon as the Contracting Party in whose territory the pursuit is taking place so requests.	Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I. General provision, Article 13 (1), (4), (5)
What ongoing supervision is required for the use of this tool?	According to Act XCII of 2012 on police cooperation convention for Southeast Europe, no supervisions required after the authorisation while the tool is being used.	Act XCII of 2012 on police cooperation convention for Southeast Europe
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	- Act XCII of 2012 on police cooperation convention for Southeast Europe - Act LXXVII of 2012 on the cooperation in the area of witness protection - Act XC of 2017 on criminal proceedings	- Act XCII of 2012 on police cooperation convention for Southeast Europe - Act LXXVII of 2012 on the cooperation in the area of witness protection - Act XC of 2017 on criminal proceedings
How is the tool defined?	- Article "The purpose of this Agreement is to develop and enhance cooperation related to witness protection between the Contracting Parties." Article 2 (1) "The national contact points of the Contracting Parties referred to in Article 10 shall directly cooperate in the area of witness protection upon written request. The competence of the national contact points shall be governed by the national legislation." - Article 10 (1)-(2) "The law enforcement authorities of the Contracting Parties designated for the witness protection shall directly cooperate in the area of witness protection programmes. The cooperation shall, in particular, include the exchange of information, assistance as regards logistics, and taking over of persons to be protected."	- Act LXXVII of 2012 on the cooperation in the area of witness protection Article 1-2 - Act XCII of 2012 on police cooperation convention for Southeast Europe Article 10 (1)-(2)
For what types of crime can the tool be used?	cross crime areas	- Act XCII of 2012 on police cooperation convention for Southeast Europe - Act LXXVII of 2012 on the cooperation in the area of witness protection - Act XC of 2017 on criminal proceedings
Does national law allow this tool to be used in cross border cases?	- Act XC of 2017 on criminal proceedings Section 122, Section 180, Section 210, Section 526 (3), Section 704: It can be used for national criminal investigation. - Act LXXVII of 2012 on the cooperation in the area of witness protection can be used for cross border criminal investigation - Act XCII of 2012 on police cooperation convention for Southeast Europe Article 10 can be used for cross border criminal investigation	- Act XC of 2017 on criminal proceedings Section 122, Section 180, Section 210, Section 526 (3), Section 704 - Act LXXVII of 2012 on the cooperation in the area of witness protection - Act XCII of 2012 on police cooperation convention for Southeast Europe Article 10
What thresholds must be passed for the use of this tool?	N/A (The Acts do not regulate the maximum term of imprisonment of crimes for which the tool can be used)	- Act XCII of 2012 on police cooperation convention for Southeast Europe Article 10 - Act LXXVII of 2012 on the cooperation in the area of witness protection - Act XC of 2017 on criminal proceedings Section 122, Section 180, Section 210, Section 526 (3), Section 704
What types of stakeholder are involved in the implementation of this tool?	- The law enforcement authorities of the Contracting Parties - Military service witness, witness, court, prosecutor, defender, defendant	- Act XCII of 2012 on police cooperation convention for Southeast Europe Article 10 (1); Act LXXVII of 2012 on the cooperation in the area of witness protection - Act XC of 2017 on criminal proceedings Section 122, Section 180, Section 210, Section 526 (3), Section 704
Which LEAs can use this tool?	It should be regulated in the Agreement signed by the Contracting Parties. Police officers	- Act LXXVII of 2012 on the cooperation in the area of witness protection - Act XCII of 2012 on police cooperation convention for Southeast Europe Article 10 - Act XCII of 2012 on police cooperation convention for Southeast Europe Article 10 (1)-(6)
What are the rules to be followed for the implementation of this tool?	- The rules can be found in Article 10 (1)-(6): (2) The cooperation shall, in particular, include the exchange of information, assistance as regards logistics, and taking over of persons to be protected. (3) An Agreement will be signed for each particular case of taking over of persons to be protected, in order for mutual rights and obligations to be regulated. (4) The person to be protected must have been placed under the witness protection programme of the requesting Contracting Party. The person to be protected will not be included in the witness protection programme of the requested Contracting Party. When taking supportive measures in	- Act LXXVII of 2012 on the cooperation in the area of witness protection - Act XC of 2017 on criminal proceedings Section 122, Section 180, Section 210, Section 526 (3), Section 704

Relevant items	Provisions	Sources used
	connection with the protection of these persons the national legislation of the requested Contracting Party shall apply accordingly. (5) In principle the requesting Contracting Party shall bear the costs of living for the persons to be protected. The requested Contracting Party shall bear the expenses for personnel and material resources for the protection of these persons. (6) For serious reasons and after having duly notified the requesting Contracting Party, the requested Contracting Party can cease the supportive measures. In this case, the requesting Contracting Party shall retake the person concerned. - Other witness protection rules can be found in Act LXXVII of 2012 on the cooperation in the area of witness protection. - Applicable rules for national criminal investigation can be found in Act XC of 2017 on criminal proceedings Section 122, Section 180, Section 210, Section 526 (3), Section 704	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	- Article 4: "Officers from the national contact point of one Contracting Party acting under this Agreement within the territory of another Contracting Party shall be subject to the instructions given by the national contact point of the host Contracting Party." Article 5: "Officers from the national contact point of one Contracting Party acting under this Agreement within the territory of another Contracting Party may use their arms, ammunition and equipment only in legitimate self-defence or in the defence of others." Article 8: "The Contracting Parties shall ensure the full confidentiality and physical protection of all information supplied by the Contracting Parties under this Agreement, by all necessary measures in accordance with their national legislation. Classified information shall be exchanged exclusively by the national contact points of the Contracting Parties." Article 9: "In individual cases, where a Contracting Party is of the opinion that the granting of a request under this Agreement may adversely affect its national security, public order, state's interests or national legislation, such Contracting Party may refuse cooperation in whole or in part or make its cooperation conditional upon specified terms while complying with other international cooperation obligations." Article 12: "The provisions of this Agreement shall apply between Member States of the European Union only in so far as they are compatible with European Union law. Should the European Union in future introduce arrangements affecting the scope of this Agreement, European Union law shall take precedence in applying the relevant provisions of this Agreement. (2) This Agreement shall not affect rights and obligations under any existing bilateral or multilateral agreements between the Contracting Parties." - Article 10 (4): "The person to be protected will not be included in the witness protection programme of the requested Contracting Party. When taking supportive measures in connection with the protection of these persons the national legislation of the requested Contracting Party shall apply accordingly." - Further national criminal investigation rules can be found in the Act SC of 2017 on criminal proceedings Section 122, 180, 210, 526, 704.	- Act LXXVII of 2012 on the cooperation in the area of witness protection - Act XCII of 2012 on police cooperation convention for Southeast Europe Article 10 (1)-(6) - Act XC of 2017 on criminal proceedings Section 122, Section 180, Section 210, Section 526 (3), Section 704
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	- No specific authorisation needed to use this tool. However an agreement must be signed by the Contracting Parties. - The use of the rule regulated in Section 526 (3), an authorisation is needed by the Single Judge or President of the Judicial Council	- Act XCII of 2012 on police cooperation convention for Southeast Europe Article 10 (1); Act LXXVII of 2012 on the cooperation in the area of witness protection - Act XC of 2017 on criminal proceedings Section 526
What ongoing supervision is required for the use of this tool?	No supervisions required to use this tool.	Act XCII of 2012 on police cooperation convention for Southeast Europe, Act XC of 2017 on criminal proceedings and Act LXXVII of 2012 on the cooperation in the area of witness protection
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Surveillance		
Relevant documents (legal and non-legal) that define the functioning of the tool	- Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Section 220; CHAPTER XXXVI. Section 215 (5)-(6); CHAPTER XXXVIII. Section 231. a),c) --> Section 232 (1),(3) - Act XCII of 2012 on Police Cooperation Convention for Southeast Europe Article 14 Cross-border Surveillance	- Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Section 220; CHAPTER XXXVI. Section 215 (5)-(6); CHAPTER XXXVIII. Section 231. a),c) --> Section 232 (1),(3) - Act XCII of 2012 on Police Cooperation Convention for Southeast Europe Article 14 Cross-border Surveillance
Specific range of application of the tool	- victim's consent for monitoring - hidden monitoring - secret surveillance of the information system	Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Section 220; CHAPTER XXXVI. Section 215 (5)-(6); CHAPTER XXXVIII. Section 231. a),c) --> Section 232 (1),(3)

Relevant items	Provisions	Sources used
	- secret surveillance of a place - cross-border surveillance	• Act XCII of 2012 on Police Cooperation Convention for Southeast Europe Article 14 Cross-border Surveillance
How is the tool defined?	- victim's consent for monitoring (The body authorised to use concealed operations means: use surveillance with the permission of the Public Prosecutor's Office and with the written consent of the victim.) - hidden monitoring (The body authorised to use concealed operations means: may be linked to the offence (a) a person, an apartment, other premises, a fenced space, a public or public place or a vehicle, or (b) the object constituting a means of tangible proof secretly observe, collect information about what has happened and record what has been detected by a technical means (hereinafter referred to as "hidden monitoring").) - secret surveillance of the information system (Under the secret surveillance of an information system, the body authorised to use the concealed operations means: secretly know the data processed in an information system with a judicial authorisation and record the detected data by technical means.) - secret surveillance of a place (secretly observe and record what has happened in the house, in other rooms, in a fenced space or on a vehicle other than a means of public transport) - Cross-border Surveillance: (Officers of one of the Contracting Parties who, as part of a criminal investigation, are keeping under surveillance in their country a person who is presumed to have participated in an extraditable criminal offence shall subject to bilateral Implementation Agreements concluded in accordance with Article 34 paragraph 1 of this Convention be authorised to continue their surveillance in the territory of another Contracting Party where the latter has authorised cross-border surveillance in response to a request for assistance made in advance.)	• Act XC of 2017 on criminal proceedings: - victim's consent for monitoring (CHAPTER XXXVII. Section 220) - hidden monitoring (CHAPTER XXXVI. Section 215 (5)-(6)) - secret surveillance of the information system (CHAPTER XXXVIII. Section 231 a); 232 (1)) - secret surveillance of a place (CHAPTER XXXVIII. Section 231 c); 232 (3)) • Act XCII of 2012 on Police Cooperation Convention for Southeast Europe Article 14 Cross-border Surveillance
For what types of crime can the tool be used?	- victim's consent for monitoring can only be used for (a) offences of usury, domestic violence or harassment, or (b) an offence which is carried out by threat. - hidden monitoring can be only used in cases associated with a criminal offence - secret surveillance of the information system, secret surveillance of a place can be only used for intentional offences punishable by a custodial sentence of up to five years or more, or intentional offences determined in Section 234 (2) and punishable by a custodial sentence of up to 3 years or more. - Cross-border surveillance: cross crime areas; should be defined in the bilateral Implementation Agreement	• Act XC of 2017 on criminal proceedings: - victim's consent for monitoring (CHAPTER XXXVII. Section 220) - hidden monitoring (CHAPTER XXXVI. Section 215 (5)-(6)) - secret surveillance of the information system (CHAPTER XXXVIII. Section 231 a); 232 (1)) CHAPTER XXXVIII. Section 234. (1)-(2)-(3) - secret surveillance of a place (CHAPTER XXXVIII. Section 231 c); 232 (3)) + CHAPTER XXXVIII. Section 234. (1)-(2)-(3) • Act XCII of 2012 on Police Cooperation Convention for Southeast Europe Article 14 Cross-border Surveillance
Does national law allow this tool to be used in cross border cases?	- victim's consent for monitoring can be used for national criminal investigation - hidden monitoring can be used for national criminal investigation - secret surveillance of the information system can be used for national criminal investigation - secret surveillance of a place can be used for national criminal investigation These tools can be also used for cross border criminal investigations as defined in the Act XC of 2017 on criminal proceedings and in the Act CLXXX of 2012 on criminal cooperation with the Member States of the European Union. - cross-border surveillance can be used for cross border criminal investigations	• Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Section 220; CHAPTER XXXVI. Section 215 (5)-(6); CHAPTER XXXVIII. Section 231. a),c) --> Section 232 (1),(3) • Act CLXXX of 2012 on criminal cooperation with the Member States of the European Union Section 2 and Section 59/A g); Section 69/E-69/H • Act XCII of 2012 on Police Cooperation Convention for Southeast Europe Article 14 Cross-border Surveillance
What thresholds must be passed for the use of this tool?	- victim's consent for monitoring can only be used for (a) offences of usury, domestic violence or harassment, or (b) an offence which is carried out by threat. - hidden monitoring can be only used in cases associated with a criminal offence - secret surveillance of the information system, secret surveillance of a place can be only used for intentional offences punishable by a custodial sentence of up to five years or more, or intentional offences determined in Section 234 (2) and punishable by a custodial sentence of up to 3 years or more such as child prostitution, child pornography, corruption offences, offences against referendum and EU citizens' initiative, sexual abuse, drug precursor abuse.. - Cross-border Surveillance: The bilateral Implementation agreements as referred to in paragraph 1 of this Article shall define the criminal offences for which the cross-border surveillance will be applicable. The Act XCII of 2012 on Police Cooperation Convention does not regulate the maximum term of imprisonment of crimes for which the tool can be used.	• Act XC of 2017 on criminal proceedings: - victim's consent for monitoring (CHAPTER XXXVII. Section 220) - hidden monitoring (CHAPTER XXXVI. Section 215 (5)-(6)) - secret surveillance of the information system (CHAPTER XXXVIII. Section 231 a); 232 (1)) + CHAPTER XXXVIII. Section 234. (1)-(2)-(3) - secret surveillance of a place (CHAPTER XXXVIII. Section 231 c); 232 (3)) + CHAPTER XXXVIII. Section 234. (1)-(2)-(3) • Act XCII of 2012 on Police Cooperation Convention for Southeast Europe Article 14 Cross-border Surveillance
What types of stakeholder are involved in the implementation of this tool?	-secret surveillance of the information system, secret surveillance of a place -- can be used by an authority which has the authorisation by the judge -victim's consent for monitoring must be authorised by the victim and the prosecutor --> the victim, the prosecutor, the authorised body - an authorised body can carry out the hidden monitoring (authorisation can be given by the judge, prosecutor, investigating authority) - Cross-border surveillance: Law enforcement authorities of the two contracting parties,	• Act XC of 2017 on criminal proceedings: - victim's consent for monitoring (CHAPTER XXXVII. Section 220) - hidden monitoring (CHAPTER XXXVI. Section 215 (5)-(6)) - secret surveillance of the information system (CHAPTER XXXVIII. Section 231 a); 232 (1)) + CHAPTER XXXVIII. Section 234. (1)-(2)-(3) - secret surveillance of a place (CHAPTER XXXVIII. Section 231 c); 232 (3)) + CHAPTER XXXVIII. Section 234. (1)-(2)-(3) • Act XCII of 2012 on Police Cooperation Convention for Southeast Europe Article 14 Cross-border Surveillance
Which LEAs can use this tool?	-secret surveillance of the information system, secret surveillance of a place -- can be used by an authority which has the authorisation by the judge -victim's consent for monitoring must be authorised by the victim and the prosecutor and can be used by an authority which has these authorisations	• Act XC of 2017 on criminal proceedings: - victim's consent for monitoring (CHAPTER XXXVII. Section 220) - hidden monitoring (CHAPTER XXXVI. Section 215 (5)-(6))

Relevant items	Provisions	Sources used
	- an authorised body can carry out the hidden monitoring (authorisation can be given by the judge, prosecutor, investigating authority) Cross-border surveillance: Officers of one of the Contracting Parties who, as part of a criminal investigation, are keeping under surveillance in their country.	- secret surveillance of the information system (CHAPTER XXXVIII. Section 231 a); 232 (1)) + CHAPTER XXXVIII. Section 234. (1)-(2)-(3) - secret surveillance of a place (CHAPTER XXXVIII. Section 231 c); 232 (3)) + CHAPTER XXXVIII. Section 234. (1)-(2)-(3) Act XCII of 2012 on Police Cooperation Convention for Southeast Europe Article 14 Cross-border Surveillance
What are the rules to be followed for the implementation of this tool?	- victim's consent for monitoring: The main rule can be found in CHAPTER XXXVII. Section 220. Other applicable rules can be found under Section 228-230. - hidden monitoring: The main rule can be found in CHAPTER XXXVI. Section 215 (5)-(6)) - secret surveillance of the information system, secret surveillance of a place: The main rule can be found in CHAPTER XXXVIII. Section 231. and Section 232 (1), (3) and Section 233-234. However, there are certain rules which must be followed by the covert operation performing authorities. These are the following: - Covert operation authorisation (Section 235-239); - Duration and extension of application (Section 239-243) - Withdraw and prohibit the covert operation (Section 242) - Implementation of covert operation (Section 243-245) - Termination of covert operation (Section 245) - Rules on data obtained in the use of covert operation (CHAPTER XL) - Results of the use of covert operation (CHAPTER XLI) -Cross-border surveillance: The authorisation rules (Act XCII of 2012 on Police Cooperation Convention for Southeast Europe Article 14 Cross-border Surveillance (1)-(2)); and the Article 14 (5) mentions the rules how the surveillance must be carried out: The officers carrying out the surveillance must comply with the provisions of this Article and with the law of the Contracting Party in whose territory they are operating; they must obey the instructions of the competent local authorities. b) Except in the situations outlined in paragraph 2, the officers shall, during the surveillance, carry a document certifying that authorisation has been granted. c) The officers carrying out the surveillance must at all times be able to prove that they are acting in an official capacity. d) The officers carrying out the surveillance may carry their service weapons during the surveillance unless specifically otherwise decided by the requested Party; their use shall be prohibited except in cases of legitimate self-defence. e) Entry into private homes and places not accessible to the public is prohibited. f) The officers carrying out the surveillance may neither challenge nor arrest the person under surveillance. g) All operations shall be the subject of a report to the authorities of the Contracting Party in whose territory they took place; the officers carrying out the surveillance may be required to appear in person. h) The authorities of the Contracting Party from which the surveillance officers have come shall, when requested by the authorities of the Contracting Party in whose territory the surveillance took place, assist the enquiry subsequent to the operation in which they took part, including judicial proceedings, provided that the identity of the involved officer is protected.	- Act XC of 2017 on criminal proceedings: - victim's consent for monitoring (CHAPTER XXXVII. Section 220 + Section 228-230) - hidden monitoring (CHAPTER XXXVI. Section 215 (5)-(6)) - secret surveillance of the information system, secret surveillance of a place (CHAPTER XXXVIII. Section 231 a), c); 232 (1), (3)) + CHAPTER XXXVIII. Section 234-245; CHAPTER XL-XLI - Act XCII of 2012 on Police Cooperation Convention for Southeast Europe Article 14 Cross-border Surveillance
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	- victim's consent for monitoring: The rules can be found in the Act of 2017 on criminal proceedings Section 220, 228-230. The monitoring can be used only for 45 days! Other relevant restrictions on data obtained in the use of covert operations can be found in CHAPTER XL. Furthermore other relevant rules on the implementation and termination of covert operations can be found in in Section243-246. - hidden monitoring: The rules can be found in Section 215 (5)- (6). Other relevant restrictions on data obtained in the use of covert operations can be found in CHAPTER XL. Furthermore other relevant rules on the implementation and termination of covert operations can be found in in Section243-246. - secret surveillance of the information system, secret surveillance of a place: The rules on Withdraw and prohibit the "secret surveillance of the information system and secret surveillance of a place" operation can be found in the Act XC of 2017 on criminal proceedings Section 242. This Section regulates the cases when the judge can withdraw the authorisation (such as: the scope of the authorisation has been exceeded, the body authorised to use concealed means does not present the data within the time limit laid down in paragraph (1)). All the cases can be found in Section 242. Other relevant restrictions on data obtained in the use of covert operations can be found in CHAPTER XL. Furthermore other relevant rules on the implementation and termination of covert operations can be found in in Section243-246. Cross-border surveillance: Some of the restrictions are regulated in Article 14 (5), as mentioned above:	- Act XC of 2017 on criminal proceedings: - victim's consent for monitoring (CHAPTER XXXVII. Section 220 + Section 228-230, Section 243-246, CHAPTER XL) - hidden monitoring (CHAPTER XXXVI. Section 215 (5)-(6), Section 243-246, CHAPTER XL) - secret surveillance of the information system, secret surveillance of a place Section 242 + CHAPTER XXXVIII. Section 234-246; CHAPTER XL-XLI - Act XCII of 2012 on Police Cooperation Convention for Southeast Europe Article 14 Cross-border Surveillance (5)

Relevant items	Provisions	Sources used
	The officers carrying out the surveillance must comply with the provisions of this Article and with the law of the Contracting Party in whose territory they are operating; they must obey the instructions of the competent local authorities. b) Except in the situations outlined in paragraph 2, the officers shall, during the surveillance, carry a document certifying that authorisation has been granted. c) The officers carrying out the surveillance must at all times be able to prove that they are acting in an official capacity. d) The officers carrying out the surveillance may carry their service weapons during the surveillance unless specifically otherwise decided by the requested Party; their use shall be prohibited except in cases of legitimate self-defence. e) Entry into private homes and places not accessible to the public is prohibited. f) The officers carrying out the surveillance may neither challenge nor arrest the person under surveillance. g) All operations shall be the subject of a report to the authorities of the Contracting Party in whose territory they took place; the officers carrying out the surveillance may be required to appear in person. h) The authorities of the Contracting Party from which the surveillance officers have come shall, when requested by the authorities of the Contracting Party in whose territory the surveillance took place, assist the enquiry subsequent to the operation in which they took part, including judicial proceedings, provided that the identity of the involved officer is protected.	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	-secret surveillance of the information system, secret surveillance of a place -- can be used by an authority which has the authorisation by the judge . According to Section 238 if the authorisation by the judge would cause such a delay that would significantly jeopardise the aim, it can be authorised by the prosecutor. In this case the prosecutor can order the covert operations for 120 hours or until the judge's decision. -victim's consent for monitoring must be authorised by the victim and the prosecutor and can be used by an authority which has the authorisation - an authorised body can carry out the hidden monitoring (authorisation can be given by the judge, prosecutor, investigating authority) - Cross-border surveillance: On request, the surveillance will be entrusted to officers of the Contracting Party in whose territory this is carried out. The request for assistance referred to in the first subparagraph must be sent to an authority designated by each of the Contracting Parties and empowered to grant or to pass on the requested authorisation. (exceptional case: Where, for particularly urgent reasons, prior request for authorisation cannot be submitted from the requesting Contracting Party, the Officers carrying out the surveillance shall subject to bilateral Implementation Agreements mentioned in paragraph 1 of this Article be allowed to continue beyond the border the surveillance of a person presumed to have committed a criminal offence as mentioned in paragraph 3.)	- Act XC of 2017 on criminal proceedings: - victim's consent for monitoring (CHAPTER XXXVII. Section 220) - hidden monitoring (CHAPTER XXXVI. Section 215 (5)-(6)) - secret surveillance of the information system (CHAPTER XXXVIII. Section 231 a); 232 (1)) + CHAPTER XXXVIII. Section 234. (1)-(2)-(3) - secret surveillance of a place (CHAPTER XXXVIII. Section 231 c); 232 (3)) + CHAPTER XXXVIII. Section 234. (1)-(2)-(3) - Act XCII of 2012 on Police Cooperation Convention for Southeast Europe Article 14 Cross-border Surveillance
What ongoing supervision is required for the use of this tool?	According to Act XC of 2017 on criminal proceedings and Act XCII of 2012 on police cooperation convention for Southeast Europe, no supervisions required after the authorisation while the tool is being used.	Act XC of 2017 on criminal proceedings and Act XCII of 2012 on police cooperation convention for Southeast Europe
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Undercover / covert operations		
Relevant documents (legal and non-legal) that define the functioning of the tool	- Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Section 216-218, Section 220; CHAPTER XXXVI. Section 215 (5)-(6); CHAPTER XXXVIII. Section 231. a)-e) --> Section 232 (1)-(5) - Act CXXV of 1995 on national security services Section 53-61 Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I, General Provision, Article 16 + Article 17	- Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Section 216-218, Section 220; CHAPTER XXXVI. Section 215 (5)-(6); CHAPTER XXXVIII. Section 231. a)-e) --> Section 232 (1)-(5) - Act CXXV of 1995 on national security services Section 53-61 - Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I, General Provision, Article 16 + Article 17
How is the tool defined?	Act XC of 2017 on criminal proceedings: - monitor payment transactions (The body authorised to use the concealed operations means: with the permission of the Public Prosecutor's Office, order the body carrying out the financial services or ancillary financial services activities provided for in the Law on Credit Institutions and Financial Undertakings (hereinafter referred to as the 'service provider') to record and retain or transfer data relating to payment transactions under the Law on the Provision of Payment Services for a specified period.)	- Act XC of 2017 on criminal proceedings: - monitor payment transactions (CHAPTER XXXVII. Section 216) - victim's consent for monitoring (CHAPTER XXXVII. Section 220) - hidden monitoring (CHAPTER XXXVI. Section 215 (5)-(6)) - secret surveillance of the information system (CHAPTER XXXVIII. Section 231 a); 232 (1)) - secret research (CHAPTER XXXVIII. Section 231 b); 232 (2)) - secret surveillance of a place (CHAPTER XXXVIII. Section 231 c); 232 (3))

Relevant items	Provisions	Sources used
	- victim's consent for monitoring (The body authorised to use concealed operations means: use surveillance with the permission of the Public Prosecutor's Office and with the written consent of the victim.) - hidden monitoring (The body authorised to use concealed operations means: may be linked to the offence (a) a person, an apartment, other premises, a fenced space, a public or public place or a vehicle, or (b) the object constituting a means of tangible proof secretly observe, collect information about what has happened and record what has been detected by a technical means (hereinafter referred to as "hidden monitoring").) - secret surveillance of the information system (Under the secret surveillance of an information system, the body authorised to use the concealed operations means: secretly know the data processed in an information system with a judicial authorisation and record the detected data by technical means.) - secret research (Under secret search, the body authorised to use concealed operations means: with the exception of a public or public place, secretly search, record an apartment, other premises, a fenced space or a vehicle, with the exception of a means of public transport, and an object in the use of the person concerned.) - secret surveillance of a place (secretly observe and record what has happened in the house, in other rooms, in a fenced space or on a vehicle other than a means of public transport) - secret knowledge of a shipment (open mail or other sealed mail in secret, get to know its contents, check it and record it.) - eavesdropping (secretly know and record the content of communications by electronic communications network or device or information system in the context of an electronic communications service.) Act CXXV of 1995 on national security services Section 53-61: - covert information gathering (National security services may, with the exception of the Counter-Terrorism Information and Crime Analysis Centre, collect secret information in order to carry out their duties under Section 4 to 9; this does not cover the performance of the tasks specified in Section 4(h) and 8(1)(d)-e).) Another definition can be found in Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I, General Provision, Article 16 (1).	- secret knowledge of a shipment (CHAPTER XXXVIII. Section 231 d); 232 (4)) - eavesdropping (CHAPTER XXXVIII. Section 231 e); 232 (5)) - covert information gathering (Act CXXV of 1995 on national security services Section 53-61) • Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I, General Provision, Article 16 (1)
For what types of crime can the tool be used?	Cross crime areas	• Act XC of 2017 on criminal proceedings: - monitor payment transactions (CHAPTER XXXVII. Section 216) - victim's consent for monitoring (CHAPTER XXXVII. Section 220) - hidden monitoring (CHAPTER XXXVI. Section 215 (5)-(6)) - secret surveillance of the information system (CHAPTER XXXVIII. Section 231 a); 232 (1)) - secret research (CHAPTER XXXVIII. Section 231 b); 232 (2)) - secret surveillance of a place (CHAPTER XXXVIII. Section 231 c); 232 (3)) - secret knowledge of a shipment (CHAPTER XXXVIII. Section 231 d); 232 (4)) - eavesdropping (CHAPTER XXXVIII. Section 231 e); 232 (5)) - covert information gathering (Act CXXV of 1995 on national security services Section 53-61)
Does national law allow this tool to be used in cross border cases?	- monitor payment transactions can be used for national criminal investigations. - victim's consent for monitoring can be used for national criminal investigations. - hidden monitoring can be used for national criminal investigations. - secret surveillance of the information system can be used for national criminal investigations. - secret research can be used for national criminal investigations. - secret surveillance of a place can be used for national criminal investigations. - secret knowledge of a shipment can be used for national criminal investigations. - eavesdropping can be used for national criminal investigations. - covert information gathering can be used for national criminal investigations. These tools can be also used for cross border criminal investigations as defined in the Act CXXV of 1995 on national security services, the Act XC of 2017 on criminal proceedings and in the Act CLXXX of 2012 on criminal cooperation with the Member States of the European Union. - Undercover Investigations to Investigate Crimes: can be used for cross border criminal investigations	• Act XC of 2017 on criminal proceedings: - monitor payment transactions (CHAPTER XXXVII. Section 216) - victim's consent for monitoring (CHAPTER XXXVII. Section 220) - hidden monitoring (CHAPTER XXXVI. Section 215 (5)-(6)) - secret surveillance of the information system (CHAPTER XXXVIII. Section 231 a); 232 (1)) - secret research (CHAPTER XXXVIII. Section 231 b); 232 (2)) - secret surveillance of a place (CHAPTER XXXVIII. Section 231 c); 232 (3)) - secret knowledge of a shipment (CHAPTER XXXVIII. Section 231 d); 232 (4)) - eavesdropping (CHAPTER XXXVIII. Section 231 e); 232 (5)) - covert information gathering (Act CXXV of 1995 on national security services Section 53-61) - Act CLXXX of 2012 on criminal cooperation with the Member States of the European Union Section 2 and Section 59/A g); Section 69/E-69/H - Undercover Investigation to Investigate Crimes: Act XCII of 2012 on Police Cooperation Convention for Southeast Europe Article 16
What thresholds must be passed for the use of this tool?	- victim's consent for monitoring can only be used for (a) offences of usury, domestic violence or harassment, or (b) an offence which is carried out by threat. There are no regulation on the maximum term of imprisonment of crimes for which the tool can be used - hidden monitoring can be only used in cases associated with a criminal offence; There are no regulations on the maximum term of imprisonment of crimes for which the tool can be used	• Act XC of 2017 on criminal proceedings: - monitor payment transactions (CHAPTER XXXVII. Section 216) - victim's consent for monitoring (CHAPTER XXXVII. Section 220) - hidden monitoring (CHAPTER XXXVI. Section 215 (5)-(6)) - secret surveillance of the information system (CHAPTER XXXVIII. Section 231 a); 232 (1)) + CHAPTER XXXVIII. Section 234. (1)-(2)-(3)

Relevant items	Provisions	Sources used
	- secret surveillance of the information system, secret research, secret surveillance of a place, secret knowledge of a shipment or eavesdropping can be only used for intentional offences punishable by a custodial sentence of up to five years or more, or intentional offences determined in Section 234 (2) and punishable by a custodial sentence of up to 3 years or more. - covert information gathering (National security services may, with the exception of the Counter-Terrorism Information and Crime Analysis Centre, collect secret information in order to carry out their duties under Section 4 to 9; this does not cover the performance of the tasks specified in Section 4(h) and 8(1)(d)-e).) The Act CXXV of 1995 on national security services Section 53-61 does not regulate the maximum term of imprisonment of crimes for which the tool can be used - Undercover Investigation to Investigate Crimes: According to the Act XCII of 2012 on Police Convention for Southeast Europe, there are no regulations on the maximum term of imprisonment of crimes for which the tool can be used.	- secret research (CHAPTER XXXVIII. Section 231 b); 232 (2)) + CHAPTER XXXVIII. Section 234. (1)-(2)-(3) - secret surveillance of a place (CHAPTER XXXVIII. Section 231 c); 232 (3)) + CHAPTER XXXVIII. Section 234. (1)-(2)-(3) - secret knowledge of a shipment (CHAPTER XXXVIII. Section 231 d); 232 (4)) + CHAPTER XXXVIII. Section 234. (1)-(2)-(3) - eavesdropping (CHAPTER XXXVIII. Section 231 e); 232 (5)) + CHAPTER XXXVIII. Section 234. (1)-(2)-(3) - covert information gathering (Act CXXV of 1995 on national security services Section 53-61) - Undercover Investigation to Investigate Crimes: Act XCII of 2012 on Police Cooperation Convention for Southeast Europe Article 16
What types of stakeholder are involved in the implementation of this tool?	- victim's consent for monitoring can only be used by and authority which has the authorisation by the victim and the prosecutor - hidden monitoring--> an authorised body can carry out the hidden monitoring (authorisation can be given by the judge, prosecutor, investigating authority) - secret surveillance of the information system, secret research, secret surveillance of a place, secret knowledge of a shipment or eavesdropping can be by an authority which has the authorisation by the judge - covert information gathering --> National security services - Undercover Investigation to Investigate Crimes: the contracting Parties, police officers	• Act XC of 2017 on criminal proceedings: - monitor payment transactions (CHAPTER XXXVII. Section 216) - victim's consent for monitoring (CHAPTER XXXVII. Section 220) - hidden monitoring (CHAPTER XXXVI. Section 215 (5)-(6)) - secret surveillance of the information system (CHAPTER XXXVIII. Section 231 a); 232 (1)) + CHAPTER XXXVIII. Section 234. (1)-(2)-(3) - secret research (CHAPTER XXXVIII. Section 231 b); 232 (2)) + CHAPTER XXXVIII. Section 234. (1)-(2)-(3) - secret surveillance of a place (CHAPTER XXXVIII. Section 231 c); 232 (3)) + CHAPTER XXXVIII. Section 234. (1)-(2)-(3) - secret knowledge of a shipment (CHAPTER XXXVIII. Section 231 d); 232 (4)) + CHAPTER XXXVIII. Section 234. (1)-(2)-(3) - eavesdropping (CHAPTER XXXVIII. Section 231 e); 232 (5)) + CHAPTER XXXVIII. Section 234. (1)-(2)-(3) - covert information gathering (Act CXXV of 1995 on national security services Section 53-61) - Undercover Investigation to Investigate Crimes: Act XCII of 2012 on Police Cooperation Convention for Southeast Europe Article 16
Which LEAs can use this tool?	- covert information gathering -- National security services -secret surveillance of the information system, secret research, secret surveillance of a place, secret knowledge of a shipment or eavesdropping -- an authority which has the authorisation by the judge - monitoring payment transactions must be authorised by the prosecutor -victim's consent for monitoring must be authorised by the victim and the prosecutor and can be used by an authority which has the authorisation - an authorised body can carry out the hidden monitoring (authorisation can be given by the judge, prosecutor, investigating authority) - Undercover Investigation to Investigate Crimes: the contracting Parties, police officers	• Act XC of 2017 on criminal proceedings: - monitor payment transactions (CHAPTER XXXVII. Section 216) - victim's consent for monitoring (CHAPTER XXXVII. Section 220) - hidden monitoring (CHAPTER XXXVI. Section 215 (5)-(6)) - secret surveillance of the information system (CHAPTER XXXVIII. Section 231 a); 232 (1)) + CHAPTER XXXVIII. Section 234. (1)-(2)-(3) - secret research (CHAPTER XXXVIII. Section 231 b); 232 (2)) + CHAPTER XXXVIII. Section 234. (1)-(2)-(3) - secret surveillance of a place (CHAPTER XXXVIII. Section 231 c); 232 (3)) + CHAPTER XXXVIII. Section 234. (1)-(2)-(3) - secret knowledge of a shipment (CHAPTER XXXVIII. Section 231 d); 232 (4)) + CHAPTER XXXVIII. Section 234. (1)-(2)-(3) - eavesdropping (CHAPTER XXXVIII. Section 231 e); 232 (5)) + CHAPTER XXXVIII. Section 234. (1)-(2)-(3) - covert information gathering (Act CXXV of 1995 on national security services Section 53-61) - Undercover Investigation to Investigate Crimes: Act XCII of 2012 on Police Cooperation Convention for Southeast Europe Article 16
What are the rules to be followed for the implementation of this tool?	-secret surveillance of the information system, secret research, secret surveillance of a place, secret knowledge of a shipment or eavesdropping: The main rule can be found in CHAPTER XXXVIII. Section 231. and Section 232-234. However, there are certain rules which must be followed by the covert operation performing authorities. These are the following: - Covert operation authorisation (Section 235-239); - Duration and extension of application (Section 239-243) - Withdraw and prohibit the covert operation (Section 242) - Implementation of covert operation (Section 243-245) - Termination of covert operation (Section 245) - Rules on data obtained in the use of covert operation (CHAPTER XL) - Results of the use of covert operation (CHAPTER XLI) - covert information gathering: The rules can be found in the Act CXXV of 1995 on national security services Section 53-61. - hidden monitoring (CHAPTER XXXVI. Section 215 (5)-(6)) - monitoring payment transactions: The main rule can be found in CHAPTER XXXVII. Section 216-218. This includes maximum duration of monitoring payment transactions (3 months+ can	-secret surveillance of the information system, secret research, secret surveillance of a place, secret knowledge of a shipment or eavesdropping: The main rule can be found in CHAPTER XXXVIII. Section 231. and Section 232-234. However, there are certain rules which must be followed by the covert operation performing authorities. These are the following: - Covert operation authorisation (Section 235-239); - Duration and extension of application (Section 239-243) - Withdraw and prohibit the covert operation (Section 242) - Implementation of covert operation (Section 243-245) - Termination of covert operation (Section 245) - Rules on data obtained in the use of covert operation (CHAPTER XL) - Results of the use of covert operation (CHAPTER XLI) - covert information gathering: The rules can be found in the Act CXXV of 1995 on national security services Section 53-61. - hidden monitoring (CHAPTER XXXVI. Section 215 (5)-(6))

Relevant items	Provisions	Sources used
	be lengthened 1 time); when it is prohibited to perform the monitoring; who can give the authorisation (the prosecutor) and what should be defined in the decision. Moreover other applicable rules for performing covert operations authorised by the prosecutor are included in Section 228-230. - victim's consent for monitoring: The main rule can be found in CHAPTER XXXVII. Section 220. Other applicable rules can be found under Section 228-230. Further rules can be found in the Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I, General Provision, Article 16 (2)-(7).	- monitoring payment transactions: The main rule can be found in CHAPTER XXXVII. Section 216-218. This includes maximum duration of monitoring payment transactions (3 months+ can be lengthened 1 time); when it is prohibited to perform the monitoring; who can give the authorisation (the prosecutor) and what should be defined in the decision. Moreover other applicable rules for performing covert operations authorised by the prosecutor are included in Section 228-230. - victim's consent for monitoring: The main rule can be found in CHAPTER XXXVII. Section 220. Other applicable rules can be found under Section 228-230. Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I, General Provision, Article 16 (2)-(7)
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	- victim's consent for monitoring: The rules can be found in the Act of 2017 on criminal proceedings Section 220, 228-230. The monitoring can be used only for 45 days! Other relevant restrictions on data obtained in the use of covert operations can be found in CHAPTER XL. Furthermore other relevant rules on the implementation and termination of covert operations can be found in in Section243-246. - hidden monitoring: The rules can be found in Section 215 (5)- (6). Other relevant restrictions on data obtained in the use of covert operations can be found in CHAPTER XL. Furthermore other relevant rules on the implementation and termination of covert operations can be found in in Section243-246. - secret surveillance of the information system, secret surveillance of a place, secret research, secret knowledge of a shipment or eavesdropping: The rules on Withdraw and prohibit the "secret surveillance of the information system, secret surveillance of a place, secret research, secret knowledge of a shipment or eavesdropping" operation can be found in the Act XC of 2017 on criminal proceedings Section 242. This Section regulates the cases when the judge can withdraw the authorisation (such as: the scope of the authorisation has been exceeded, the body authorised to use concealed means does not present the data within the time limit laid down in paragraph (1)). All the cases can be found in Section 242. Other relevant restrictions on data obtained in the use of covert operations can be found in CHAPTER XL. Furthermore other relevant rules on the implementation and termination of covert operations can be found in in Section243-246. - monitoring payment transactions: The main rule can be found in CHAPTER XXXVII. Section 216-218. This includes maximum duration of monitoring payment transactions (3 months+ can be lengthened 1 time); when it is prohibited to perform the monitoring; who can give the authorisation (the prosecutor) and what should be defined in the decision. Moreover other applicable rules for performing covert operations authorised by the prosecutor are included in Section 228-230. Other relevant restrictions on data obtained in the use of covert operations can be found in CHAPTER XL. Furthermore other relevant rules on the implementation and termination of covert operations can be found in in Section243-246. - covert information gathering: The rules can be found in the Act CXXV of 1995 on national security services Section 53-61. -Undercover Investigation to Investigate Crimes: The rules can be found in Act XCII of 2012 on police cooperation convention for Southeast Europe Article 16. According to Article 16 (2) "Undercover investigations on the territory of the requested Contracting Party shall be restricted to single, temporary operations. Preparations of these operations shall be done by way of coordination between the officers involved from the Contracting Parties. The deployment of an undercover investigator and the execution of the actions taken by the undercover investigator shall be managed by the requested Contracting Party. The requested Contracting Party is responsible for the action taken by an undercover investigator of the requesting Contracting Party, and can, at any time, demand the termination of the operation."	- victim's consent for monitoring: Act of 2017 on criminal proceedings Section 220, 228-230 and Section 243-246 and CHAPTER XL - hidden monitoring: Act of 2017 on criminal proceedings Section215 (5)-(6) and Section 243-246 and CHAPTER XL - secret surveillance of the information system, secret surveillance of a place, secret research, secret knowledge of a shipment or eavesdropping: Act of 2017 on criminal proceedings Section 242 and Section 243-246 and CHAPTER XL - monitoring payment transactions: Act of 2017 on criminal proceedings Section 216-218, 228-230 and Section 243-246 and CHAPTER XL - covert information gathering: Act CXXV of 1995 on national security services Section 53-61 - Undercover Investigation to Investigate Crimes: Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I, General Provision, Article 16 (2)
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	- covert information gathering -- National security services -secret surveillance of the information system, secret research, secret surveillance of a place, secret knowledge of a shipment or eavesdropping -- it must be authorised by the judge. According to Section 238 if the authorisation by the judge would cause such a delay that would significantly jeopardise the aim, it can be authorised by the prosecutor. In this case the prosecutor can order the covert operations for 120 hours or until the judge's decision. - monitoring payment transactions must be authorised by the prosecutor -victim's consent for monitoring must be authorised by the victim and the prosecutor - an authorised body can carry out the hidden monitoring (authorisation can be given by the judge, prosecutor, investigating authority) Preparations of these operations shall be done by way of coordination between the officers involved from the Contracting Parties.	- Act XC of 2017 on criminal proceedings: - monitor payment transactions (CHAPTER XXXVII. Section 216) - victim's consent for monitoring (CHAPTER XXXVII. Section 220) - hidden monitoring (CHAPTER XXXVI. Section 215 (5)-(6)) - secret surveillance of the information system (CHAPTER XXXVIII. Section 231 a); 232 (1)) + CHAPTER XXXVIII. Section 234. (1)-(2)-(3) - secret research (CHAPTER XXXVIII. Section 231 b); 232 (2)) + CHAPTER XXXVIII. Section 234. (1)-(2)-(3) - secret surveillance of a place (CHAPTER XXXVIII. Section 231 c); 232 (3)) + CHAPTER XXXVIII. Section 234. (1)-(2)-(3) - secret knowledge of a shipment (CHAPTER XXXVIII. Section 231 d); 232 (4)) + CHAPTER XXXVIII. Section 234. (1)-(2)-(3) - eavesdropping (CHAPTER XXXVIII. Section 231 e); 232 (5)) + CHAPTER XXXVIII. Section 234. (1)-(2)-(3) - covert information gathering (Act CXXV of 1995 on national security services Section 53-61)

Relevant items	Provisions	Sources used
What ongoing supervision is required for the use of this tool?	According to Act XC of 2017 on criminal proceedings, Act XCII of 2012 on police cooperation convention for Southeast Europe and Act CXXV of 1995 on national security services, no supervisions required after the authorisation while the tool is being used.	- Act XCII of 2012 on police cooperation convention for Southeast Europe, CHAPTER I, General Provision, Article 16 (2) - Act XC of 2017 on criminal proceedings, Act XCII of 2012 on police cooperation convention for Southeast Europe and Act CXXV of 1995 on national security services
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Section 222-226; CHAPTER XXXIX. Implementation of the use of covert operations Section 243; CHAPTER XLI. Section Results of the use of covert operations Section 255	Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Section 222-226; CHAPTER XXXIX. Implementation of the use of covert operations Section 243; CHAPTER XLI. Section Results of the use of covert operations Section 255
Specific range of application of the tool	Act CXXII of 2010 on the National Tax and Customs Administration Section 53 - Member of the public - Victim of a crime - Other member of the authorised body	- Act CXXII of 2010 on the National Tax and Customs Administration Section 53 - Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Section 222-226; CHAPTER XXXIX. Implementation of the use of covert operations Section 243; CHAPTER XLI. Section Results of the use of covert operations Section 256 - Act CXXII of 2010 on the National Tax and Customs Administration Section - Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Section 222 - Act CXXII of 2010 on the National Tax and Customs Administration Section 52 e)
How is the tool defined?	A body authorised to use concealed means may employ a member of the authorised body (hereinafter referred to as the 'undercover investigator') who is permanently concealing his or her belongings or identity and who is specifically employed to carry out such a task in criminal proceedings with the permission of the Public Prosecutor's Office. Act CXXII of 2010 on the National Tax and Customs Administration Section 52 e) "The NAV body authorized to conduct covert information gathering operations shall carry out such operations: e) for the protection of a financial investigation officer employed to operate undercover on the long term, concealing his/her true identity and association with the NAV (hereinafter referred to as "undercover detective"), ... "Act CXXII of 2010 on the National Tax and Customs Administration Section 52 e) "The NAV body authorised to conduct covert information gathering operations shall carry out such operations: e) for the protection of a financial investigation officer employed to operate undercover on the long term, concealing his/her true identity and association with the NAV (hereinafter referred to as "undercover detective"), .."	
For what types of crime can the tool be used?	Cross crime areas Act CXXII of 2010 on the National Tax and Customs Administration Section 52-55 : Financial crimes	- Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Section 222 (2) - Act CXXII of 2010 on the National Tax and Customs Administration Section 52-55
Does national law allow this tool to be used in cross border cases?	The use of informants, regulated in Act CXXII of 2010 on the National Tax and Customs Administration Section 52-55 and Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Section 222 (2), can be used for national criminal investigations. However it can be also used for cross border criminal investigations as defined in the Act CXXII of 2010 on the National Tax and Customs Administration, Act XC of 2017 on criminal proceedings and in the Act CLXXX of 2012 on criminal cooperation with the Member States of the European Union.	Act XC of 2017 on criminal proceedings; Act CXXII of 2010 on the National Tax and Customs Administration, Act CLXXX of 2012 on criminal cooperation with the Member States of the European Union Section 2 and Section 59/A g); Section 69/E-69/H
What thresholds must be passed for the use of this tool?	Undercover Investigator is applicable for the purposes of (a) infiltration into a criminal organisation, (b) infiltration into a terrorist group or an organisation supplying or collecting material means to provide the conditions for an act of terrorism, or providing material support for the commission of an act of terrorism or the activities of a terrorist group by providing material means or otherwise supporting the activities of a terrorist group, (c) sham purchases, (d) carrying out hidden monitoring, (e) the transmission of information pursuant to Article 215(7), or (f) obtaining information and evidence relating to the offence. There are no specific rules on the maximum term of imprisonment of crimes for which the tool can be used. There are no specific rules on the maximum term of imprisonment of crimes for which the tool can be used.	- Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Section 222 (2) - Act CXXII of 2010 on the National Tax and Customs Administration Section 52-55
What types of stakeholder are involved in the implementation of this tool?	The prosecutor, the authorised person as a undercover investigator The use of informants in Section 52 e) of Act CXXII of 2010 on the National Tax and Customs Administration: "for the protection of a financial investigation officer employed to operate undercover on the long term, concealing his/her true identity and association with the NAV (hereinafter referred to as "undercover detective"), or any organisation operating under disguise (hereinafter referred to as "front organisation")," --> the NAV; and the authorised undercover detective or front organisation	- Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Section 222 - Act CXXII of 2010 on the National Tax and Customs Administration Section 52 e)
Which LEAs can use this tool?	It can be used by those authorised by the prosecutor.	- Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Section 222 - Act CXXII of 2010 on the National Tax and Customs Administration Section 52 e) and Section 54 b)

Relevant items	Provisions	Sources used
	The use of informants in Section 52 e) and Section 54 of Act CXXII of 2010 on the National Tax and Customs Administration: "The NAV body authorised to conduct covert information gathering operations shall be entitled, for the purposes defined in Section 52: to work together with a financial investigation officer who operates undercover, or with an undercover detective for gathering or verifying information, without revealing the true aim of these actions;" This rule is regulated under the Means for Which No Court Order is Required. So only the NAV authorisation need for using this tool.	
What are the rules to be followed for the implementation of this tool?	The main rule can be found in Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Section 222-226. Undercover investigator can participate in sham purchases which rule can be found in Section 226. Moreover other rules connected to the authorisation process can be found in Section 228-230 and Section 255. Furthermore the implementation of covert operations can be found in CHAPTER XXXIX. Section 243-244. Section 53 of Act CXXII of 2010 on the National Tax and Customs Administration: Covert information gathering operations may be carried out for the protection of an undercover detective or front organisation where reasonable grounds exist to believe that it will yield information: a) for protecting the undercover detective from the risks of detection, or for preventing any violent crime against the undercover detective, or b) for protecting the front organisation from the risks of detection. Section 55 of Act CXXII of 2010 on the National Tax and Customs Administration:(1) An undercover detective shall not be prosecuted for any criminal or misdemeanour offense, or any infraction punishable by an administrative penalty committed while working undercover, if: a) it is alleged to be necessary for the success of the operation, for achieving the objectives provided for in Section 52, and the objective intended to be achieved supersedes the reason for prosecuting the undercover detective, b) it is alleged to be necessary for protecting the undercover detective from the risks of detection or for ensuring his safety, and the need for protecting the undercover detective from the risks of detection or for ensuring his safety supersedes the reason for prosecuting the undercover detective, and/or c) it is alleged to be necessary for the prevention or interception of another crime, and the need for the prevention or interception of that crime supersedes the reason for prosecuting the undercover detective. (2) An undercover detective shall not assault another person with intent to commit murder, and shall not commit any crime resulting in permanent disability or serious health impairment of another person. (3) An undercover detective shall not incite another person to commit a crime, and shall not steer the person affected towards committing a crime of greater gravity as the one originally intended. (4) If the undercover detective cannot not be prosecuted pursuant to Subsection (1) for a criminal or misdemeanour offense, or an infraction punishable by an administrative penalty he has committed, the State shall provide compensation or restitution for which the undercover detective would be liable under civil law. In connection with the provision of said compensation or restitution, the NAV body authorised to conduct covert information gathering operations may move to conclude a non-disclosure agreement with the aggrieved party, and/or may prepare the documents required for such an agreement. (5) If compensation or restitution is to be awarded by way of civil action, the legal basis for such claims shall be presumed. In civil actions the State is represented by the minister in charge of the judicial system. Before delivering its decision, the court hearing the civil action shall move to obtain a statement from the NAV body authorised to conduct covert information gathering operations concerning the offense committed against the plaintiff, the resulting damage and violation of rights relating to personality. The statement may not reveal any fact from which the identity of the undercover detective may be inferred.	- Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Section 222-226; Section 228-230 and 255; Section 243-244. - Act CXXII of 2010 on the National Tax and Customs Administration Section 51-57
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Use of informants, regulated in the Act XC on criminal proceedings,: The restrictions can be found in CHAPTER XXXII. Section 222-226 (such as: Section 224. (3)-(4): "An undercover investigator shall not commit a crime involving the intentional loss of another person's life or intentionally causing permanent disability or serious deterioration of health."; "An undercover detective shall not assault another person with intent to commit murder, and shall not commit any crime resulting in permanent disability or serious health impairment of another person. An undercover detective shall not incite another person to commit a crime, and shall not steer the person affected towards committing a crime of greater gravity as the one originally intended"). Other relevant restrictions on data obtained in the use of covert operations can be found in CHAPTER XL. Furthermore other relevant rules on the implementation and termination of covert operations can be found in in Section243-246. - Section 51 (4): "In the interest of detecting and preventing criminal activities, for the identification and apprehension of the perpetrator, for obtaining evidence and for recovering criminal assets, the NAV may use covert means defined in the Act XC of 2017 on criminal proceeding.";	- Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Section 224, Section 243-246 and regulations in CHAPTER XL - Act CXXII of 2010 on the National Tax and Customs Administration Section 51-57

Relevant items	Provisions	Sources used
	- Section 53/A: "For the involvement, supervision and protection of persons who secretly collaborate with the NAV, and persons who secretly collaborate under the Code of Criminal Proceedings, and for the verification of information provided by such persons means for which court order is required may not be used." - Section 55 (2)-(3): "An undercover detective shall not assault another person with intent to commit murder, and shall not commit any crime resulting in permanent disability or serious health impairment of another person. An undercover detective shall not incite another person to commit a crime, and shall not steer the person affected towards committing a crime of greater gravity as the one originally intended." - Section 57 (4) "The cover document shall be destroyed, and the fictitious data shall be deleted from the public register when it is no longer necessary."	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	It can be used by someone which has the authorisation by the prosecutor. According to Section 228, the prosecutor shall make the decision on enabling the covert operation within 72 hours. If the authorisation by the prosecutor would cause such a delay which would significantly jeopardise the covert operation's aim, the authorised body can start the covert operation until the prosecutor's decision. (Section 229) The use of undercover detective in Section 54 of Act CXXII of 2010 on the National Tax and Customs Administration is under the Means for Which No Court Order is Required CHAPTER, which means the authorisation can be given by the NAV.	- Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Section 222, Section 229 - Act CXXII of 2010 on the National Tax and Customs Administration Section 54
What ongoing supervision is required for the use of this tool?	According to Act XC of 2017 on criminal proceedings and Act CXXII of 2010 on the National Tax and Customs Administration, no supervisions required after the authorisation while the tool is being used.	Act XC of 2017 on criminal proceedings and Act CXXII of 2010 on the National Tax and Customs Administration
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Sham purchase		
Relevant documents (legal and non-legal) that define the functioning of the tool	Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Covert Operations for which the authorisation of the prosecutor is required Section 221 -- Sham purchase	Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Covert Operations for which the authorisation of the prosecutor is required Section 221 -- Sham purchase
How is the tool defined?	Sham purchase	Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Covert Operations for which the authorisation of the prosecutor is required Section 221 -- Sham purchase
For what types of crime can the tool be used?	Cross crime areas	Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Covert Operations for which the authorisation of the prosecutor is required Section 221 -- Sham purchase
Does national law allow this tool to be used in cross-border cases?	It can be used for national investigations and for cross border criminal investigations as defined in the Act XC of 2017 on criminal proceedings and in the Act CLXXX of 2012 on criminal cooperation with the Member States of the European Union.	- Act XC of 2017 on criminal proceedings - Act CLXXX of 2012 on criminal cooperation with the Member States of the European Union Section 2 and Section 59/A g); Section 69/E-69/H
What thresholds must be passed for the use of this tool?	With the permission of the Prosecution, a sham agreement may be concluded and performed for (a) the acquisition of a thing or its sample, or the use of a service likely to be linked to the offence, (b) the acquisition or use of a service resulting in a material means of proof of the offence with the purpose to strengthen the seller's confidence, (c) the acquisition of a thing or the use of a service in order to apprehend the perpetrator or to provide a material means of proof of the offence. There are no regulations on the maximum term of imprisonment of crimes for which the tool can be used.	Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Covert Operations for which the authorisation of the prosecutor is required Section 221 -- Sham purchase
What types of stakeholder are involved in the implementation of this tool?	The prosecutor, the authorised body or person(s).	Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Covert Operations for which the authorisation of the prosecutor is required Section 221 -- Sham purchase
Which LEAs can use this tool?	It can be used by those authorised by the prosecutor.	Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Covert Operations for which the authorisation of the prosecutor is required Section 221 -- Sham purchase
What are the rules to be followed for the implementation of this tool?	Sham purchase: The main rule can be found in Section 221. However other applicable rules can be found in Sections 226 and 228-230.	Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Section 221 -- Sham purchase+ Section 228-230
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	The main rule can be found in Section 221. Other relevant restrictions on data obtained in the use of covert operations can be found in CHAPTER XL. Furthermore other relevant rules on the implementation and termination of covert operations can be found in in Section 243-246.	Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Section 221 -- Section 243-246 and CHAPTER XL
What authorisation is needed for the use of this tool?(e.g. senior police officer, prosecutor, judge, other)	It can be used by those authorised by the prosecutor. According to Section 228, the prosecutor shall make the decision on enabling the covert operation within 72 hours. If the authorisation by the prosecutor would cause such a delay which would significantly jeopardise the covert	Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Covert Operations for which the authorisation of the prosecutor is required Section 221 -- Sham purchase, Section 228-229

Relevant items	Provisions	Sources used
	operation's aim, the authorised body can start the covert operation until the prosecutor's decision. (Section 229)	
What ongoing supervision is required for the use of this tool?	According to Act XC of 2017 on criminal proceedings, no supervisions required after the authorisation while the tool is being used.	Act XC of 2017 on criminal proceedings CHAPTER XXXVII. Covert Operations for which the authorisation of the prosecutor is required Section 221 -- Sham purchase, Section 228-229
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	

Source: Author's own elaboration

Iceland

Table 31 – Overview of national rules on investigative tools - Iceland

Relevant items	Provisions	Sources used
Controlled Delivery		
Relevant documents (legal and non-legal) that define the functioning of the tool	- Regulation on special methods and police action in criminal investigations. (<i>Chapter IV. Supervised delivery</i>)	(Chapter IV "Afhending undir eftirliti.") https://www.reglugerd.is/reglugerdir/eftir-raduneytum/innanrikisraduneyti/nr/17692
How is the tool defined?	Supervised delivery means postponing seizure, but being under constant surveillance, drug shipment or other illegal or suspicious shipment on the way to the country, around the country or out of the country. The purpose of supervised delivery is to inform the consignee of the consignment, the methods of transport and the possible distribution system, thus obtaining evidence of criminal conduct.	- Chapter IV "Afhending undir eftirliti." - nr. 15 ("Skilgreining og markmið.") https://www.reglugerd.is/reglugerdir/eftir-raduneytum/innanrikisraduneyti/nr/17692
For what types of crime can the tool be used?	In order to use special methods and actions of the police that is outlined in the regulation, a condition that is listed ne must be met, unless otherwise stated in the regulation. The general condition is that there need to be reasoned suspicion that a serious offense is being committed, or that an attempt will be made to commit a serious offense, which may result in a minimum of eight years' imprisonment. So all type of crimes can apply as long as they could result in eight years imprisonment. The regulation list some other crimes that also apply no matter the minimum years imprison it the offence is violation of some article in law on criminal conduct (Lög um almennarhegningar no 19/1940) and some other special laws. Among that is: Drugs, Financial crimes, Responsible for the spread of susceptible diseases as a part of an organised crime, Sexual offenses against a child, Prostitution and enrichment offense	See article. nr. 3. (Skilyrði) in the regulation.
Does national law allow this tool to be used in cross border cases?	The National Commissioner of Police may authorize law enforcement officers of other states to monitor the delivery under supervision in Icelandic territory, provided that they have the required permits from the authorities in their home state. However, they do not have police power. The National Commissioner of Police may authorize Icelandic police officers to monitor delivery under supervision outside Icelandic territory and to work under the direction of foreign law enforcement authorities during the operation.	- Chapter IV "Afhending undir eftirliti." - nr. 19 ("Störf löggæslumanna utan heimaríkis.") https://www.reglugerd.is/reglugerdir/eftir-raduneytum/innanrikisraduneyti/nr/17692
What thresholds must be passed for the use of this tool?	The regulations does not specify any "maximum terms", only minimum terms of eight years of imprisonment (with some expectation to specific crimes where no terms of imprisonments does apply).	
What types of stakeholder are involved in the implementation of this tool?	LEAs	https://www.reglugerd.is/reglugerdir/eftir-raduneytum/innanrikisraduneyti/nr/17692
Which LEAs can use this tool?	Icelandic Police	- Chapter IV "Afhending undir eftirliti." - nr. 16 ("Ákvörðun og stjórn.") https://www.reglugerd.is/reglugerdir/eftir-raduneytum/innanrikisraduneyti/nr/17692
What are the rules to be followed for the implementation of this tool?	Delivery under supervision may take place at the request of a foreign country, provided that the following conditions are met: 1. Technical equipment and manpower are available to ensure uninterrupted control of the shipment during the operation.	- Chapter IV "Afhending undir eftirliti." - nr. 17 ("Skilyrði.") https://www.reglugerd.is/reglugerdir/eftir-raduneytum/innanrikisraduneyti/nr/17692 - Chapter IV "Afhending undir eftirliti." - nr. 22 ("Aðgerð fer fram innanlands.")

Relevant items	Provisions	Sources used
	2. It has been examined whether it is possible to change the contents of the consignment, e.g. drugs, in whole or in part. In the case of supervised delivery that is transferred between countries with a stopover in Iceland (i.e. transit), the conditions are also set that the final destination is known, the relevant foreign authorities ensure uninterrupted control of the shipment, that it is seized and those involved will be prosecuted. The National Commissioner of Police may, with the approval of the State Prosecutor, prescribe supervision of a shipment between two or more districts of the National Commissioner of Police. The provisions of these rules shall then apply as appropriate.	• https://www.reglugerd.is/reglugerdir/eftir-raduneytum/innanrikisraduneyti/nr/17692
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool?	The National Commissioner of Police decides on delivery under supervision. He may also request co-operation with the law enforcement authorities of other states.	• Chapter IV "Afhending undir eftirliti." - nr. 16 ("Ákvörðun og stjórn.") • https://www.reglugerd.is/reglugerdir/eftir-raduneytum/innanrikisraduneyti/nr/17692
What ongoing supervision is required for the use of this tool?	Before the National Commissioner of Police decides that a delivery under supervision takes place in this country or seeks co-operation with the law enforcement authorities of other states, he must notify the State Prosecutor and the Director of Customs.	• Chapter IV "Afhending undir eftirliti." - nr. 16 ("Ákvörðun og stjórn.") • https://www.reglugerd.is/reglugerdir/eftir-raduneytum/innanrikisraduneyti/nr/17692
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Data available on the number of times this tool has been used for SOC cases	N/A	
Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	No specific regulation or law, based on comment from Icelandic police the rules about emergency driving 643/2004 does apply for this and some internal procedures that are not public on the internet.	• Reglur um neyðarakstur 643/2004 • https://www.samgongustofa.is/media/log-og-reglur-i-umferdarmalum/643_2004.pdf
How is the tool defined?	Vehicles may only be driven in accordance with the rules on emergency driving if the driving is considered necessary for police operations, for rescuing people, for ambulances, for fires, for environmental accidents or a traffic accident or to prevent significant damage and that the vehicle is registered for emergency driving, (Article 2 - Paragraph 2 - Registration and recognition.) The provision for the registration of a vehicle for emergency driving does not, however, apply to police vehicles, which as a rule are used for surveillance or similar tasks but in exceptional cases used for emergency driving, and vehicles that are occasionally used for driving in the service of the police, fire brigade or for vital purposes, such as transporting a sick person person or injured, (Paragraph 3 Article 8 of the Traffic Act.) Vehicles of the Presidency, Parliament and Ministries, already accompanied by the police, in connection with official visits may be subject to these rules without being specifically registered for such driving.	• Reglur um neyðarakstur 643/2004 (Article 1 1. gr. "Neyðarakstur") • https://www.samgongustofa.is/media/log-og-reglur-i-umferdarmalum/643_2004.pdf
For what types of crime can the tool be used?	Police operations, for rescuing people, for ambulances, for fires, for environmental accidents or a traffic accident or to prevent significant damage	
Does national law allow this tool to be used in cross border cases?	Does not apply for Iceland	
What thresholds must be passed for the use of this tool?	The regulations does not specify any "maximum terms", only minimum terms of eight years of imprisonment (with some expectation to specific crimes where no terms of imprisonments does apply).	
What types of stakeholder are involved in the implementation of this tool?	LEAs	
Which LEAs can use this tool?	Icelandic police	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Samgöngustofa (Transportation office) registers vehicles for emergency driving. Vehicles must have previously been approved for their use by an inspection or by specific approval, in the case of an ambulance. Police, fire brigade and civil protection vehicles can be registered for emergency driving. Vehicles of other public authorities, as well as ambulances, rescue vehicles and similar vehicles, even if	• Reglur um neyðarakstur 643/2004 (Article 2. . "Skráning og viðurkenning.") • https://www.samgongustofa.is/media/log-og-reglur-i-umferdarmalum/643_2004.pdf • Reglur um neyðarakstur 643/2004 (Article 3. "Ökutæki sem skrá má.")

Relevant items	Provisions	Sources used
	they are privately owned, may be registered for emergency driving, with the permission of the Ministry of Transport.	• https://www.samgongustofa.is/media/log-og-reglur-i-umferdarmalum/643_2004.pdf
What ongoing supervision is required for the use of this tool?	the permission of the Ministry of Transport.	• Reglur um neyðarakstur 643/2004 (Article 3. "Ökutæki sem skrá má.") • https://www.samgongustofa.is/media/log-og-reglur-i-umferdarmalum/643_2004.pdf
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	No specific regulation or law for Witness protection. The only thing we found about the subject where found in the Criminal law (Article nr. 65)	• https://www.althingi.is/lagas/nuna/2008088.html
How is the tool defined?	A witness may request that his name, ID number and home, as well as other information that could indicate his whereabouts, not be included in a police report, if he considers that there is a danger to the life, health or liberty of himself or his close relatives	• Article nr. 65 • https://www.althingi.is/lagas/nuna/2008088.html
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	Icelandic police	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Surveillance		
Relevant documents (legal and non-legal) that define the functioning of the tool	- Regulation on special methods and police action in criminal investigations. (Chapter V. Shading)	• (Chapter IV "Skygging.") • https://www.reglugerd.is/reglugerdir/eftir-raduneytum/innanrikisraduneyti/nr/17692
Specific range of application of the tool	Shading shall, as a general rule, be the police officer's detention of a dwelling or other demarcated area or monitoring of the movements of the person suspected of a crime, including the pursuit of a vehicle or other vehicle. Traffic rules according to the rules on emergency driving apply as applicable. Recording of images and sound in places other than those specified in the second paragraph. Article 82 Act on Criminal Procedure, no. 88/2008, is not permitted except according to a court ruling. The same applies if other special techniques are used to monitor human movements in places not covered by the second paragraph. Article 82 of the Act.	• Chapter IV "Skygging." - nr. 24 ("Framkvæmd") • https://www.reglugerd.is/reglugerdir/eftir-raduneytum/innanrikisraduneyti/nr/17692

Relevant items	Provisions	Sources used
How is the tool defined?	Shading is an investigative measure that involves constantly monitoring the movement of people through housing or in another demarcated area or in public places by monitoring the movements of the person suspected of a crime. The purpose of shadowing is to inform who is suspected of having committed a criminal offense, obtain information about travel and communication and thus obtain evidence of criminal conduct.	- Chapter IV "Skygging." - nr. 23 ("Skilgreining og markmið.") https://www.reglugerd.is/reglugerdir/eftir-raduneytum/innanrikisraduneyti/nr/17692
For what types of crime can the tool be used?	In order to use special methods and actions of the police that is outlined in the regulation, a condition that is listed ne must be met, unless otherwise stated in the regulation. The general condition is that there need to be reasoned suspicion that a serious offense is being committed, or that an attempt will be made to commit a serious offense, which may result in a minimum of eight years' imprisonment. So all type of crimes can apply as long as they could result in eight years imprisonment. The regulation list some other crimes that also apply no matter the minimum years imprison it the offence is violation of some article in law on criminal conduct (Lög um almennarhegningar no 19/1940) and some other special laws. Among that is: Drugs, Financial crimes, Responsible for the spread of susceptible diseases as a part of an organised crime, Sexual offenses against a child, Prostitution and enrichment offense	See article. nr. 3. (Skilyrði) in the regulation.
Does national law allow this tool to be used in cross border cases?	N/A	- Chapter IV "Skygging." - nr. 19 ("Störf löggæslumanna utan heimáðs.") https://www.reglugerd.is/reglugerdir/eftir-raduneytum/innanrikisraduneyti/nr/17692
What thresholds must be passed for the use of this tool?	The regulations does not specify any "maximum terms", only minimum terms of eight years of imprisonment (with some expectation to specific crimes where no terms of imprisonments does apply).	
What types of stakeholder are involved in the implementation of this tool?	LEAs	https://www.reglugerd.is/reglugerdir/eftir-raduneytum/innanrikisraduneyti/nr/17692
Which LEAs can use this tool?	Icelandic police	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Undercover / covert operations		
Relevant documents (legal and non-legal) that define the functioning of the tool	- Regulation on special methods and police action in criminal investigations (Chapter VI other methods (Undercover)) - Regulation on special methods and police action in criminal investigations. (Chapter V. No 25 "Flugumenn")	- Chapter IV "Skygging." - nr. 23 ("Skilgreining og markmið.") https://www.reglugerd.is/reglugerdir/eftir-raduneytum/innanrikisraduneyti/nr/17692
How is the tool defined?	The police may, with the approval of the representative of a company or institution, use as disguise work clothes, vehicles or other identified objects of a company or institution for the purpose of a criminal investigation. The police may, under the same conditions, have a police officer disguised as taking a position within the territory of a company or institution, including participating in the activities of a company or institution as if it were an employee, without the knowledge of other employees or the person being investigated. "Flugumenn" is a police officer or other police officer who exercises police authority, Icelandic or foreign, and takes a position within a group of people suspected of being responsible for a serious criminal activity and provides the police with information about the activities and the people connected to them.	- Chapter IV "Skygging." - nr. 23 ("Skilgreining og markmið.") https://www.reglugerd.is/reglugerdir/eftir-raduneytum/innanrikisraduneyti/nr/17692

Relevant items	Provisions	Sources used
For what types of crime can the tool be used?	In order to use special methods and actions of the police that is outlined in the regulation, a condition that is listed ne must be met, unless otherwise stated in the regulation. The general condition is that there need to be reasoned suspicion that a serious offense is being committed, or that an attempt will be made to commit a serious offense, which may result in a minimum of eight years' imprisonment. So all type of crimes can apply as long as they could result in eight years imprisonment. The regulation list some other crimes that also apply no matter the minimum years imprison it the offence is violation of some article in law on criminal conduct (Lög um almennarhegningar no 19/1940) and some other special laws. Among that is: Drugs, Financial crimes, Responsible for the spread of susceptible diseases as a part of an organised crime, Sexual offenses against a child, Prostitution and enrichment offense	See article. nr. 3. (Skilyrði) in the regulation.
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	The regulations does not specify any "maximum terms", only minimum terms of eight years of imprisonment (with some expectation to specific crimes where no terms of imprisonments does apply).	
What types of stakeholder are involved in the implementation of this tool?	LEAs	
Which LEAs can use this tool?	Icelandic police.	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	- Regulation on special methods and police action in criminal investigations. (<i>Chapter III. Use of informants</i>)	Regulation on special methods and actions of the police in criminal investigations. (Chapter III. Uppljóstrarar) https://www.reglugerd.is/reglugerdir/eftir-raduneytum/innanrikisraduneyti/nr/17692 https://www.reglugerd.is/reglugerdir/eftir-raduneytum/innanrikisraduneyti/nr/17692
Specific range of application of the tool	The regulations mention two types of informants in Chapter III. - Member of the public - Other police officers	https://www.reglugerd.is/reglugerdir/eftir-raduneytum/innanrikisraduneyti/nr/17692
How is the tool defined?	The investigative measures provided for in these rules are called special methods and actions of the police in criminal investigations. They aim to prevent, investigate and obtain all available evidence of criminal conduct and to search for the suspect in a crime, all in such a way that the person being investigated is not aware of the investigation.	https://www.reglugerd.is/reglugerdir/eftir-raduneytum/innanrikisraduneyti/nr/17692
For what types of crime can the tool be used?	In order to use special methods and actions of the police that is outlined in the regulation, a condition that is listed ne must be met, unless otherwise stated in the regulation. The general condition is that there need to be reasoned suspicion that a serious offense is being committed, or that an attempt will be made to commit a serious offense, which may result in a minimum of eight years' imprisonment. So all type of crimes can apply as long as they could result in eight years imprisonment. The regulation list some other crimes that also apply no matter the minimum years imprison it the offence is violation of some article in law on criminal conduct (Lög um almennarhegningar no 19/1940) and some other special laws. Among that is: Drugs, Financial crimes, Responsible for the spread of susceptible diseases as a part of an organised crime, Sexual offenses against a child, Prostitution and enrichment offense	- See article. nr. 3. (Skilyrði) in the regulation. https://www.reglugerd.is/reglugerdir/eftir-raduneytum/innanrikisraduneyti/nr/17692
Does national law allow this tool to be used in cross border cases?	The regulations does not specify any conditions regarding national investigation or cross border.	https://www.reglugerd.is/reglugerdir/eftir-raduneytum/innanrikisraduneyti/nr/17692

Relevant items	Provisions	Sources used
What thresholds must be passed for the use of this tool?	The regulations does not specify any "maximum terms", only minimum terms of eight years of imprisonment (with some expectation to specific crimes where no terms of imprisonments does apply).	• https://www.reglugerd.is/reglugerdir/eftir-raduneytum/innanrikisraduneyti/nr/17692
What types of stakeholder are involved in the implementation of this tool?	LEAs	• https://www.reglugerd.is/reglugerdir/eftir-raduneytum/innanrikisraduneyti/nr/17692
Which LEAs can use this tool?	Icelandic police.	• https://www.reglugerd.is/reglugerdir/eftir-raduneytum/innanrikisraduneyti/nr/17692
What are the rules to be followed for the implementation of this tool?	The crime needs to fulfil requirement listed in "For what types of crime can the tool be used?" but additionally there need to be reason to believe that information obtained in this way can be of great importance for the investigation of the case. It must be assumed that other methods will not be sufficient to obtain such information. Investigative measures under these rules will not be applied if they result in criminal conduct that would not otherwise have been committed. The application of this methods shall always be proportionate.	• See article. nr. 3. (Skilyrði) in the regulation. • https://www.reglugerd.is/reglugerdir/eftir-raduneytum/innanrikisraduneyti/nr/17692
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Investigative measures under these rules will not be applied if they result in criminal conduct that would not otherwise have been committed. The application of this methods shall always be proportionate. When the method and action of the police according to these rules have been completed, the police shall notify the person to whom the action is directed about it without delay, however, so that it does not harm further investigation of the case.	• See article. nr. 3. (Skilyrði) in the regulation. • See article. nr. 5. (Ákvörðun) in the regulation. • https://www.reglugerd.is/reglugerdir/eftir-raduneytum/innanrikisraduneyti/nr/17692
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	A decision on the application of special methods and actions of the police shall be made by the chief of police or another officer nominated by the chief of police.	• See article. nr. 6. (Ákvörðun) in the regulation. • https://www.reglugerd.is/reglugerdir/eftir-raduneytum/innanrikisraduneyti/nr/17692
What ongoing supervision is required for the use of this tool?	The Office of the Public Prosecutor supervises the implementation of methods and actions according to these regulation. Chiefs of Police shall notify the Office of the Public Prosecutor of the application of methods and measures pursuant to the regulation as soon as possible.	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	

Source: Author's own elaboration

Ireland

Table 32 – Overview of national rules on investigative tools - Ireland

Relevant items	Provisions	Sources used
Controlled Delivery		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Justice (Mutual Assistance) Act (2008) Section 88	• Criminal Justice (Mutual Assistance) Act (2008) Section 88: http://www.irishstatutebook.ie/eli/2008/act/7/section/88/enacted/en/html
How is the tool defined?	Criminal Justice (Mutual Assistance) Act (2008) Section 88 states: "controlled delivery" means a delivery permitted in the State in accordance with this Chapter or in a designated state in accordance with the relevant international instrument for the purposes of an investigation into an offence;' "controlled drug" has the meaning given to it by section 2 of the Misuse of Drugs Act 1977 ; "offence" includes an offence which is suspected, with reasonable cause, to have been or to be about to be committed.	• Criminal Justice (Mutual Assistance) Act (2008) Section 88: http://www.irishstatutebook.ie/eli/2008/act/7/section/88/enacted/en/html
For what types of crime can the tool be used?	Drugs and revenue offences are mentioned in Criminal Justice (Mutual Assistance) Act (2008) Section 88, however this may not be an extensive list of when controlled delivery is permitted The document does not give a full list of which offences controlled delivery is permitted in, so it is possible that it may be used in a wider range of crimes.	• Criminal Justice (Mutual Assistance) Act (2008) Section 88: http://www.irishstatutebook.ie/eli/2008/act/7/section/88/enacted/en/html
Does national law allow this tool to be used in cross border cases?	Yes, controlled delivery is permitted within designated states. Criminal Justice (Mutual Assistance) Act (2008) Section 88 states "controlled delivery" means a delivery permitted in the State in accordance with this Chapter or in a designated state in accordance with the relevant international instrument for the purposes of an investigation into an offence;'	• Criminal Justice (Mutual Assistance) Act (2008) Section 88: http://www.irishstatutebook.ie/eli/2008/act/7/section/88/enacted/en/html
What thresholds must be passed for the use of this tool?	points 4a and 4b related specifically to the use of controlled delivery for drug offences Certain regulations must be met in order for controlled delivery to be used as per Criminal Justice (Mutual Assistance) Act (2008): 90.— '(1) This section applies to a request to the Competent Authority in the State from a competent authority in a designated state to permit— (a) a controlled delivery to be made in the State, and	• Criminal Justice (Mutual Assistance) Act (2008) Section 90: http://www.irishstatutebook.ie/eli/2008/act/7/section/90/enacted/en/html

Relevant items	Provisions	Sources used
	(b) specified persons, or persons of a specified description, from the designated state to participate in the operations connected with the controlled delivery. (2) The request shall include particulars of the offence with which the controlled delivery is concerned. (3) The Competent Authority in the State may grant the request if satisfied that— (a) the controlled delivery is being made for the purposes of an investigation into an offence, or (b) there are reasonable grounds for believing that it is in the public interest, having regard to the benefit likely to accrue to the investigation, to permit the delivery to take place. (4) The operations related to a controlled delivery shall, if the delivery is concerned with the illegal importation of controlled drugs, be regulated in accordance with— (a) the Memorandum of Understanding of 12 January 1996 concerning the relationship between the Customs and Excise Service of the Revenue Commissioners and the Garda Síochána with respect to Drugs Law Enforcement and agreed between the Commissioner of the Garda Síochána and the chairman of the Revenue Commissioners, and (b) the Operational Protocol for co-operation between An Garda Síochána, the Customs and Excise and the Naval Service in relation to Drugs Law Enforcement, including any modifications or extensions of the Memorandum or Protocol for the time being in force. (5) If the delivery is concerned with a revenue offence (other than an offence constituted by the illegal importation of controlled drugs), the operations shall be under the direction and control of the officers of customs and excise assigned to the delivery. (6) If the delivery is concerned with any other offence, the operations shall be under the direction and control of the members of the Garda Síochána so assigned. (7) A member of the Garda Síochána or officer of customs and excise participating in operations connected with a controlled delivery in the State may, at the request of a person from a designated state so participating, take such action as may be open to the member or officer in furtherance of the operations. (8) Copies of the Memorandum of Understanding and Operational Protocol have been placed in the Oireachtas Library.' No mention is made of maximum terms of imprisonment	
What types of stakeholder are involved in the implementation of this tool?	"Competent Authority in the State" - either Commissioner of the Garda Síochána or a member of the Garda Síochána authorised by him or her - makes the request for a controlled delivery or If the controlled delivery is concerned with a revenue offence, the Revenue Commissioners - makes the request for a controlled delivery. A judicial authority - where the competent authority of a designated state requires requests under this Chapter to be received or made by a judicial authority, the requests shall be addressed to or made by the Minister. "Minister" means the Minister for Justice, Equality and Law Reform Specified persons or persons of a specified description, including members of the Garda Síochána and officers of customs and excise, to participate in the operations connected with the delivery. If the delivery is concerned with a revenue offence (other than an offence constituted by the illegal importation of controlled drugs), the operations shall be under the direction and control of the officers of customs and excise assigned to the delivery. If the delivery is concerned with any other offence, the operations shall be under the direction and control of the members of the Garda Síochána so assigned.	Criminal Justice (Mutual Assistance) Act (2008) Section 88-90: http://www.irishstatutebook.ie/eli/2008/act/7/section/88/enacted/en/html
Which LEAs can use this tool?	If the delivery is concerned with a revenue offence (other than an offence constituted by the illegal importation of controlled drugs), the operations shall be under the direction and control of the officers of customs and excise assigned to the delivery. If the delivery is concerned with any other offence, the operations shall be under the direction and control of the members of the Garda Síochána so assigned.	Criminal Justice (Mutual Assistance) Act (2008) Section 90: http://www.irishstatutebook.ie/eli/2008/act/7/section/90/enacted/en/html
What are the rules to be followed for the implementation of this tool?	Certain regulations must be met in order for controlled delivery to be used: 90.— '(1) This section applies to a request to the Competent Authority in the State from a competent authority in a designated state to permit— (a) a controlled delivery to be made in the State, and (b) specified persons, or persons of a specified description, from the designated state to participate in the operations connected with the controlled delivery. (2) The request shall include particulars of the offence with which the controlled delivery is concerned. (3) The Competent Authority in the State may grant the request if satisfied that— (a) the controlled delivery is being made for the purposes of an investigation into an offence, or (b) there are reasonable grounds for believing that it is in the public interest, having regard to the benefit likely to accrue to the investigation, to permit the delivery to take place. (4) The operations related to a controlled delivery shall, if the delivery is concerned with the illegal importation of controlled drugs, be regulated in accordance with— (a) the Memorandum of Understanding of 12 January 1996 concerning the relationship between the Customs and Excise Service of the Revenue Commissioners and the Garda Síochána with	Criminal Justice (Mutual Assistance) Act (2008) Section 90: http://www.irishstatutebook.ie/eli/2008/act/7/section/90/enacted/en/html

Relevant items	Provisions	Sources used
	respect to Drugs Law Enforcement and agreed between the Commissioner of the Garda Síochána and the chairman of the Revenue Commissioners, and (b) the Operational Protocol for co-operation between An Garda Síochána, the Customs and Excise and the Naval Service in relation to Drugs Law Enforcement, including any modifications or extensions of the Memorandum or Protocol for the time being in force. (5) If the delivery is concerned with a revenue offence (other than an offence constituted by the illegal importation of controlled drugs), the operations shall be under the direction and control of the officers of customs and excise assigned to the delivery. (6) If the delivery is concerned with any other offence, the operations shall be under the direction and control of the members of the Garda Síochána so assigned. (7) A member of the Garda Síochána or officer of customs and excise participating in operations connected with a controlled delivery in the State may, at the request of a person from a designated state so participating, take such action as may be open to the member or officer in furtherance of the operations. (8) Copies of the Memorandum of Understanding and Operational Protocol have been placed in the Oireachtas Library.'	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool?	As described above	• Criminal Justice (Mutual Assistance) Act (2008) Section 90: http://www.irishstatutebook.ie/eli/2008/act/7/section/90/enacted/en/html • Criminal Justice (Mutual Assistance) Act (2008) Section 90: http://www.irishstatutebook.ie/eli/2008/act/7/section/90/enacted/en/html
What ongoing supervision is required for the use of this tool?	(5) If the delivery is concerned with a revenue offence (other than an offence constituted by the illegal importation of controlled drugs), the operations shall be under the direction and control of the officers of customs and excise assigned to the delivery. (6) If the delivery is concerned with any other offence, the operations shall be under the direction and control of the members of the Garda Síochána so assigned.	• https://www.casemine.com/judgement/uk/5da046024653d07b2518fa5b#
Is there any national case law relating to the use of this tool in cross-border crime cases?	Director of Public Prosecutions v Twesigye, 13/05/2015, court of appeal relating to conviction on 17/12/2013 where the defendant was charged with possession of a controlled drug and possession of a controlled drug for the purposes of selling it or otherwise supplying it to another after controlled delivery used following discovery of drugs at customs. The court did not uphold the ground of appeal.	
Data available on the number of times this tool has been used for SOC cases	N/A	
Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	N/A	
How is the tool defined?	N/A	
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	

Relevant items	Provisions	Sources used
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	There is currently no legislative framework for witness protection in Ireland, however, the Criminal Justice Act, 1999 Section 40 discusses relocated witnesses with regards to it being an offence to disclose to attempt to discover their whereabouts.	Criminal Justice (Mutual Assistance) Act 2008: http://www.irishstatutebook.ie/eli/2008/act/7/section/13/enacted/en/html
How is the tool defined?	(3) In this section "relocated witness" means any person who intends to give or has given evidence in proceedings for an offence and who as a consequence has moved residence, under any programme operated by the Garda Síochána for the protection of witnesses, to any place, whether within or outside the State.	- Criminal Justice (Mutual Assistance) Act 2008: http://www.irishstatutebook.ie/eli/2008/act/7/section/14/enacted/en/html http://www.irishstatutebook.ie/eli/2008/act/7/section/15/enacted/en/html
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	As per, Criminal Justice Act, 1999 Section 40.—(1) A person who without lawful authority makes enquiries or takes any other steps whatever, whether within or outside the State, for the purpose of discovering— (a) the whereabouts of a person whom he or she knows, or reasonably suspects, to be a relocated witness, or (b) any new name or other particulars related to any new identity provided for such a witness, shall be guilty of an offence. (2) A person who without lawful authority discloses, whether within or outside the State, to any other person any information (including information lawfully obtained pursuant to subsection (1)) concerning— (a) the whereabouts of a person whom he or she knows, or reasonably suspects, to be a relocated witness, or (b) any new name or other particulars related to any new identity provided for such a person, shall be guilty of an offence.	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Surveillance		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Justice (Surveillance) Act 2009	Criminal Justice (Surveillance) Act 2009 http://www.irishstatutebook.ie/eli/2009/act/19/enacted/en/html
Specific range of application of the tool	Visual and audio surveillance is used, Criminal Justice (Surveillance) Act 2009 Section 1 says: (a) monitoring, observing, listening to or making a recording of a particular person or group of persons or their movements, activities and communications, or (b) monitoring or making a recording of places or things. Tracking surveillance is also used, Criminal Justice (Surveillance) Act 2009 Section 8 says that: a member of the Garda Síochána, a member of the Defence Forces or an officer of the Revenue Commissioners may, for a period of not more than 4 months or such shorter period as the Minister	Criminal Justice (Surveillance) Act 2009 Section 1 http://www.irishstatutebook.ie/eli/2009/act/19/section/1/enacted/en/html

Relevant items	Provisions	Sources used
	may prescribe by regulations, monitor the movements of persons, vehicles or things using a tracking device if that use has been approved by a superior officer in accordance with this section. The Act does not go into further details on specifics of the audio, visual and tracking surveillance techniques which are permitted, and does not make mention of data surveillance.	
How is the tool defined?	Criminal Justice (Surveillance) Act 2009 Section 1 defines surveillance: "surveillance" means— (a) monitoring, observing, listening to or making a recording of a particular person or group of persons or their movements, activities and communications, or (b) monitoring or making a recording of places or things, by or with the assistance of surveillance devices;	Criminal Justice (Surveillance) Act 2009 Section 1 http://www.irishstatutebook.ie/eli/2009/act/19/section/1/enacted/en/html
For what types of crime can the tool be used?	The Criminal Justice (Surveillance) Act 2009, does not go into detail about specific types of crime investigation where surveillance can be used, however Section 4 talks broadly about 'arrestable offences', so would assume surveillance can be used in cross crime areas. 4.— (1) A superior officer of the Garda Síochána may apply to a judge for an authorisation where he or she has reasonable grounds for believing that— (a) as part of an operation or investigation being conducted by the Garda Síochána concerning an arrestable offence, the surveillance being sought to be authorised is necessary for the purposes of obtaining information as to whether the offence has been committed or as to the circumstances relating to the commission of the offence, or obtaining evidence for the purposes of proceedings in relation to the offence, (b) the surveillance being sought to be authorised is necessary for the purpose of preventing the commission of arrestable offences, or (c) the surveillance being sought to be authorised is necessary for the purpose of maintaining the security of the State. (2) A superior officer of the Defence Forces may apply to a judge for an authorisation where he or she has reasonable grounds for believing that the surveillance being sought to be authorised is necessary for the purpose of maintaining the security of the State. (3) A superior officer of the Revenue Commissioners may apply to a judge for an authorisation where he or she has reasonable grounds for believing that— (a) as part of an operation or investigation being conducted by the Revenue Commissioners concerning a revenue offence, the surveillance being sought to be authorised is necessary for the purpose of obtaining information as to whether the offence has been committed or as to the circumstances relating to the commission of the offence, or obtaining evidence for the purpose of proceedings in relation to the offence, or (b) the surveillance being sought to be authorised is necessary for the purpose of preventing the commission of revenue offences.	The Criminal Justice (Surveillance) Act 2009 Section 4 http://www.irishstatutebook.ie/eli/2009/act/19/section/4/enacted/en/html
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	No mention of specific types of crime, however thresholds are mentioned in relation of arrestable offences and revenue offences in Criminal Justice (Surveillance) Act 2009 Section 4: 4.— (1) A superior officer of the Garda Síochána may apply to a judge for an authorisation where he or she has reasonable grounds for believing that— (a) as part of an operation or investigation being conducted by the Garda Síochána concerning an arrestable offence, the surveillance being sought to be authorised is necessary for the purposes of obtaining information as to whether the offence has been committed or as to the circumstances relating to the commission of the offence, or obtaining evidence for the purposes of proceedings in relation to the offence, (b) the surveillance being sought to be authorised is necessary for the purpose of preventing the commission of arrestable offences, or (c) the surveillance being sought to be authorised is necessary for the purpose of maintaining the security of the State. (2) A superior officer of the Defence Forces may apply to a judge for an authorisation where he or she has reasonable grounds for believing that the surveillance being sought to be authorised is necessary for the purpose of maintaining the security of the State. (3) A superior officer of the Revenue Commissioners may apply to a judge for an authorisation where he or she has reasonable grounds for believing that— (a) as part of an operation or investigation being conducted by the Revenue Commissioners concerning a revenue offence, the surveillance being sought to be authorised is necessary for the purpose of obtaining information as to whether the offence has been committed or as to the circumstances relating to the commission of the offence, or obtaining evidence for the purpose of proceedings in relation to the offence, or (b) the surveillance being sought to be authorised is necessary for the purpose of preventing the commission of revenue offences. No mention of maximum term of imprisonment	The Criminal Justice (Surveillance) Act 2009 Section 4 http://www.irishstatutebook.ie/eli/2009/act/19/section/4/enacted/en/html

Relevant items	Provisions	Sources used
What types of stakeholder are involved in the implementation of this tool?	Criminal Justice (Surveillance) Act 2009 Section 4, 5 and 6 mentions the following actors: Members of the Garda Síochána, members of the Defence Forces and officers of the Revenue Commissioners - carrying out of surveillance. A superior officer of the Garda Síochána, a superior officer of the Defence Forces or a superior officer of the Revenue Commissioners - makes the application for surveillance to a judge. A judge - approves or denies the application for surveillance	Criminal Justice (Surveillance) Act 2009 Section 4, 5 and 6 http://www.irishstatutebook.ie/eli/2009/act/19/enacted/en/html
Which LEAs can use this tool?	The Garda Síochána, Defence Forces and the Revenue Commissioners are permitted to use surveillance	Criminal Justice (Surveillance) Act 2009 Section 4 http://www.irishstatutebook.ie/eli/2009/act/19/section/4/enacted/en/html
What are the rules to be followed for the implementation of this tool?	The following sections of the Criminal Justice (Surveillance) Act 2009 discuss the rules to be respected when using this tool: 4.— (1) A superior officer of the Garda Síochána may apply to a judge for an authorisation where he or she has reasonable grounds for believing that— (a) as part of an operation or investigation being conducted by the Garda Síochána concerning an arrestable offence, the surveillance being sought to be authorised is necessary for the purposes of obtaining information as to whether the offence has been committed or as to the circumstances relating to the commission of the offence, or obtaining evidence for the purposes of proceedings in relation to the offence, (b) the surveillance being sought to be authorised is necessary for the purpose of preventing the commission of arrestable offences, or (c) the surveillance being sought to be authorised is necessary for the purpose of maintaining the security of the State. (2) A superior officer of the Defence Forces may apply to a judge for an authorisation where he or she has reasonable grounds for believing that the surveillance being sought to be authorised is necessary for the purpose of maintaining the security of the State. (3) A superior officer of the Revenue Commissioners may apply to a judge for an authorisation where he or she has reasonable grounds for believing that— (a) as part of an operation or investigation being conducted by the Revenue Commissioners concerning a revenue offence, the surveillance being sought to be authorised is necessary for the purpose of obtaining information as to whether the offence has been committed or as to the circumstances relating to the commission of the offence, or obtaining evidence for the purpose of proceedings in relation to the offence, or (b) the surveillance being sought to be authorised is necessary for the purpose of preventing the commission of revenue offences. (4) In a case in which surveillance carried out under section 7 is sought under subsection (10) of that section to be continued by application under this section, the information on oath supporting the application shall include a copy of the written record of approval concerned, a summary of the results of the surveillance carried out and the reasons why continued surveillance is required. (5) A superior officer who makes an application under subsection (1), (2), (3) or (4) shall also have reasonable grounds for believing that the surveillance being sought to be authorised is— (a) the least intrusive means available, having regard to its objectives and other relevant considerations, (b) proportionate to its objectives, having regard to all the circumstances including its likely impact on the rights of any person, and (c) of a duration that is reasonably required to achieve its objectives. 5.— (1) An application under section 4 for an authorisation and under section 6 for a variation or renewal of an authorisation— (a) shall be made ex parte and shall be heard otherwise than in public, and (b) may be made to a judge assigned to any district court district. (2) Subject to subsection (4), the judge shall issue such authorisation as he or she considers reasonable, if satisfied by information on oath of the superior officer concerned that— (a) the requirements specified in subsection (1), (2) or (3), as the case may be, of section 4 are fulfilled, and (b) to do so is justified, having regard to the matters referred to in section 4 (5) and all other relevant circumstances. (3) An information on oath of a superior officer specifying the grounds for his or her belief that the surveillance is necessary for the purpose of preventing the commission of arrestable offences referred to in section 4 (1) (b), or the commission of revenue offences referred to in section 4 (3) (b), need not specify a particular arrestable offence or a particular revenue offence, as the case may be, in respect of which the authorisation is being sought. (4) The judge shall not issue an authorisation if he or she is satisfied that the surveillance being sought to be authorised is likely to relate primarily to communications protected by privilege. (5) An authorisation may impose such conditions in respect of the surveillance authorised as the judge considers appropriate. (6) An authorisation shall be in writing and shall specify—	- Criminal Justice (Surveillance) Act 2009 - Criminal Justice (Surveillance) Act 2009 http://www.irishstatutebook.ie/eli/2009/act/19/enacted/en/html

Relevant items	Provisions	Sources used
	(a) particulars of the surveillance device that is authorised to be used, (b) the person who, or the place or thing that, is to be the subject of the surveillance, (c) the name of the superior officer to whom it is issued, (d) the conditions (if any) subject to which the authorisation is issued, and (e) the date of expiry of the authorisation. (7) An authorisation may authorise the superior officer named in it, or any member of the Garda Síochána, any member of the Defence Forces or any officer of the Revenue Commissioners designated by that superior officer, accompanied by any other person whom he or she considers necessary, to enter, if necessary by the use of reasonable force, any place for the purposes of initiating or carrying out the authorised surveillance, and withdrawing the authorised surveillance device, without the consent of a person who owns or is in charge of the place. (8) An authorisation shall expire on the day fixed by the judge that he or she considers reasonable in the circumstances and that is not later than 3 months from the day on which it is issued. (9) Subject to any conditions imposed by the judge under subsection (5), an authorisation shall have effect both within the district court district to which the judge is assigned and in any other part of the State. 7. (5) An approval under this section permits the member or officer concerned, accompanied by any other person whom he or she considers necessary, to enter, if necessary by the use of reasonable force, any place for the purposes of initiating or carrying out the approved surveillance, and withdrawing the approved surveillance device, without the consent of a person who owns or is in charge of the place. (6) A superior officer who approves the carrying out of surveillance under this section shall, as soon as practicable and, in any case, not later than 8 hours after the surveillance has been approved, prepare a written record of approval of that surveillance. (7) A written record of approval shall be in such form as the relevant Minister may prescribe by regulations and shall include— (a) particulars of the surveillance device that is approved to be used, (b) the person who, or the place or thing that, is to be the subject of the surveillance, (c) the name of the member of the Garda Síochána, member of the Defence Forces or officer of the Revenue Commissioners to whom the approval is granted, (d) the conditions (if any) subject to which the approval is granted, (e) the time at which the approval is granted, and (f) the duration of the approved surveillance. (8) The member or officer shall not carry out surveillance under this section for a period of more than 72 hours from the time at which the approval is granted. (9) The superior officer who approved the carrying out of surveillance may vary that approval, or any condition attached to it, at any time before the expiry of the period of 72 hours. (10) (a) If the superior officer who approved the carrying out of surveillance believes on reasonable grounds that surveillance beyond the period of 72 hours is warranted, he or she shall, as soon as possible but in any case before the expiry of that period, make an application under section 4 (4) for an authorisation to continue the surveillance. (b) Where an application under section 4 (4) has been made and the period referred to in paragraph (a) would, but for this paragraph, expire during the hearing of the application, it shall be deemed not to expire until the determination of the application. (11) A superior officer who approves the carrying out of surveillance under this section shall make a report as soon as possible and, in any case, not later than 7 days after the surveillance concerned has been completed, specifying the grounds on which the approval was granted, and including a copy of the written record of approval and a summary of the results of the surveillance. (12) A report under subsection (11) shall be made to— (a) in the case of a member of the Garda Síochána, a member of the Garda Síochána of the rank of Assistant Commissioner, (b) in the case of an officer of the Defence Forces, a general officer within the meaning of section 2 > (as amended by section 2 (b) of the Defence (Amendment) Act 1979) of the Defence Act 1954 , and (c) in the case of an officer of the Revenue Commissioners, an officer of the Revenue Commissioners of the rank of Assistant Secretary. 8.— (1) Notwithstanding sections 4 to 7 , a member of the Garda Síochána, a member of the Defence Forces or an officer of the Revenue Commissioners may, for a period of not more than 4 months or such shorter period as the Minister may prescribe by regulations, monitor the movements of persons, vehicles or things using a tracking device if that use has been approved by a superior officer in accordance with this section. (2) A member or officer referred to in subsection (1) may apply to a superior officer for the grant of an approval to use a tracking device if he or she believes on reasonable grounds that—	

Relevant items	Provisions	Sources used
	(a) the requirements of subsection (1), (2) or (3), as the case may be, of section 4 are fulfilled and that surveillance is justified having regard to the matters referred to in paragraphs (b) and (c) of section 4 (5), but that the use of a tracking device would be sufficient for obtaining the information or evidence in the circumstances concerned, and (b) the information or evidence sought could reasonably be obtained by the use of a tracking device for a specified period that is as short as is practicable to allow the information or evidence to be obtained. (3) A superior officer to whom an application under subsection (2) is made shall approve such use of a tracking device as he or she considers appropriate, having regard to the information in the application, if he or she is satisfied that there are reasonable grounds for believing that an authorisation would be issued under section 5 and that the conditions specified in subsection (2) apply. (4) An approval may be granted subject to conditions, including as to the duration of the use of the tracking device. (5) An approval under this section permits the member or officer concerned, accompanied by any other person whom he or she considers necessary, to place the tracking device and remove it at the end of its use, without the consent of a person who owns or is in charge of the vehicle or thing on which it is placed. (6) A superior officer who approves the use of a tracking device under this section shall, as soon as practicable and, in any case, not later than 8 hours after the use has been approved, prepare a written record of approval of the use of the tracking device. (7) A written record of approval shall be in such form as the relevant Minister may prescribe by regulations and shall include— (a) particulars of the tracking device that is approved to be used, (b) the person who, or the vehicle or thing that, is to be monitored, (c) the name of the member of the Garda Síochána, member of the Defence Forces or officer of the Revenue Commissioners to whom the approval is granted, (d) the conditions (if any) subject to which the approval is granted, (e) the time at which the approval is granted, and (f) the duration of the use approved. (8) Without prejudice to the maximum period for which an approval granted under this section may have effect, the superior officer who approves the use of a tracking device under this section may vary that approval, or any condition attached to it, at any time before the expiry of that approval. (9) A superior officer who approves the use of a tracking device under this section shall make a report as soon as possible and, in any case, not later than 7 days after its use has ended, specifying the grounds on which the approval was granted, and including a copy of the written record of approval and a summary of the results of the monitoring. (10) A report under subsection (9) shall be made to— (a) in the case of a member of the Garda Síochána, a member of the Garda Síochána of the rank of Assistant Commissioner, (b) in the case of an officer of the Defence Forces, a general officer within the meaning of section 2 (as amended by section 2 (b) of the Defence (Amendment) Act 1979) of the Defence Act 1954, and (c) in the case of an officer of the Revenue Commissioners, an officer of the Revenue Commissioners of the rank of Assistant Secretary. 9.— (1) An application for an authorisation under section 4 or 6 , and any documents supporting the application, shall be retained until— (a) the day that is 3 years after the day on which the authorisation concerned ceases to be in force, or (b) the day on which they are no longer required for any prosecution or appeal to which they are relevant, whichever is later. (2) A written record of approval prepared under section 7 (6) or 8 (6), and a report made under section 7 (11) or 8 (9), shall be retained until— (a) the day that is 3 years after the day on which the written record of approval is prepared or the report concerned is made, or (b) the day on which they are no longer required for any prosecution or appeal to which they are relevant, whichever is later. (3) The documents obtained as a result of surveillance carried out or tracking devices used under this Act, other than those referred to in subsections (1) and (2), shall be retained until— (a) the day that is 3 years after the end of the surveillance or monitoring concerned, or (b) the day on which they are no longer required for any prosecution or appeal to which they are relevant, whichever is later.	

Relevant items	Provisions	Sources used
	(4) Subject to subsection (5), the documents referred to in subsections (1) to (3) shall be destroyed as soon as practicable after they are no longer required to be retained under those subsections. 10.— (1) The relevant Minister shall ensure that information and documents to which this Act applies are stored securely and that only persons who he or she authorises for that purpose have access to them. (2) In the interests of the protection of the privacy and other rights of persons, the security of the State, and the aims of preventing the commission of, and detecting, arrestable offences, the relevant Minister may make regulations prescribing— (a) the persons or categories of persons who are to have access for the purposes of this section to information with respect to the existence of authorisations, approvals granted under sections 7 and 8 and documents referred to in section 9 , (b) the procedures and arrangements for the secure storage, and the maintenance of the security, of that information and those documents, and (c) the number of copies that may be made of those documents and the destruction of those copies as soon as possible after they are no longer required under section 9 . (3) Notwithstanding section 13 , the Minister may make regulations respecting the disclosure or non-disclosure, to the person who was its subject or other persons whose interests are materially affected by it, of the existence of an authorisation or an approval under section 7 or 8 , provided that any disclosure authorised by such regulations is— (a) consistent with the purposes for which the authorisation or approval concerned was issued or granted, (b) consistent with the security of the State, the protection of persons' privacy and other rights and the aims of preventing and detecting the commission of arrestable offences, and (c) unlikely to hinder the investigation in the future of such offences. (4) Any regulation made under subsection (3) may— (a) require consultation by the Minister, in any particular case of disclosure, with such classes of persons as may be prescribed, (b) prescribe categories of persons (other than the subjects of the authorisations or approvals) whose interests are materially affected by authorisations or approvals, to whom disclosure is to be made, and (c) permit the imposition of terms and conditions limiting the extent or detail of disclosure as necessary, having regard to the matters referred to in subsection (3).	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	(4) For the avoidance of doubt, it is hereby declared that this Act does not apply to the following: (a) the use of a closed circuit television system in a Garda Síochána station; (b) the recording by electronic or other similar means under section 27 of the Criminal Justice Act 1984 of the questioning of a person by members of the Garda Síochána at Garda Síochána stations or elsewhere in connection with the investigation of offences; (c) the recording by electronic or other similar means of any evidence given, or statement made, by a person for the purposes of any court proceedings. 10.— (1) The relevant Minister shall ensure that information and documents to which this Act applies are stored securely and that only persons who he or she authorises for that purpose have access to them. (2) In the interests of the protection of the privacy and other rights of persons, the security of the State, and the aims of preventing the commission of, and detecting, arrestable offences, the relevant Minister may make regulations prescribing— (a) the persons or categories of persons who are to have access for the purposes of this section to information with respect to the existence of authorisations, approvals granted under sections 7 and 8 and documents referred to in section 9 , (b) the procedures and arrangements for the secure storage, and the maintenance of the security, of that information and those documents, and (c) the number of copies that may be made of those documents and the destruction of those copies as soon as possible after they are no longer required under section 9 .	Criminal Justice (Surveillance) Act 2009 Section 2 and 10 http://www.irishstatutebook.ie/eli/2009/act/19/section/2/enacted/en/html
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	A judge must approve requests for surveillance, as detailed in Criminal Justice (Surveillance) Act 2009: 3.— A member of the Garda Síochána, a member of the Defence Forces or an officer of the Revenue Commissioners shall carry out surveillance only in accordance with a valid authorisation or an approval 4.— (1) A superior officer of the Garda Síochána may apply to a judge for an authorisation where he or she has reasonable grounds for believing that— (a) as part of an operation or investigation being conducted by the Garda Síochána concerning an arrestable offence, the surveillance being sought to be authorised is necessary for the purposes of obtaining information as to whether the offence has been committed or as to the circumstances relating to the commission of the offence, or obtaining evidence for the purposes of proceedings in relation to the offence,	Criminal Justice (Surveillance) Act 2009 Section 3-5 http://www.irishstatutebook.ie/eli/2009/act/19/section/3/enacted/en/html

Relevant items	Provisions	Sources used
	(b) the surveillance being sought to be authorised is necessary for the purpose of preventing the commission of arrestable offences, or (c) the surveillance being sought to be authorised is necessary for the purpose of maintaining the security of the State. (2) A superior officer of the Defence Forces may apply to a judge for an authorisation where he or she has reasonable grounds for believing that the surveillance being sought to be authorised is necessary for the purpose of maintaining the security of the State. (3) A superior officer of the Revenue Commissioners may apply to a judge for an authorisation where he or she has reasonable grounds for believing that— (a) as part of an operation or investigation being conducted by the Revenue Commissioners concerning a revenue offence, the surveillance being sought to be authorised is necessary for the purpose of obtaining information as to whether the offence has been committed or as to the circumstances relating to the commission of the offence, or obtaining evidence for the purpose of proceedings in relation to the offence, or (b) the surveillance being sought to be authorised is necessary for the purpose of preventing the commission of revenue offences. (4) In a case in which surveillance carried out under section 7 is sought under subsection (10) of that section to be continued by application under this section, the information on oath supporting the application shall include a copy of the written record of approval concerned, a summary of the results of the surveillance carried out and the reasons why continued surveillance is required. (5) A superior officer who makes an application under subsection (1), (2), (3) or (4) shall also have reasonable grounds for believing that the surveillance being sought to be authorised is— (a) the least intrusive means available, having regard to its objectives and other relevant considerations, (b) proportionate to its objectives, having regard to all the circumstances including its likely impact on the rights of any person, and (c) of a duration that is reasonably required to achieve its objectives. 5.— (1) An application under section 4 for an authorisation and under section 6 for a variation or renewal of an authorisation— (a) shall be made ex parte and shall be heard otherwise than in public, and (b) may be made to a judge assigned to any district court district. (2) Subject to subsection (4), the judge shall issue such authorisation as he or she considers reasonable, if satisfied by information on oath of the superior officer concerned that— (a) the requirements specified in subsection (1), (2) or (3), as the case may be, of section 4 are fulfilled, and (b) to do so is justified, having regard to the matters referred to in section 4 (5) and all other relevant circumstances. (3) An information on oath of a superior officer specifying the grounds for his or her belief that the surveillance is necessary for the purpose of preventing the commission of arrestable offences referred to in section 4 (1) (b), or the commission of revenue offences referred to in section 4 (3) (b), need not specify a particular arrestable offence or a particular revenue offence, as the case may be, in respect of which the authorisation is being sought. (4) The judge shall not issue an authorisation if he or she is satisfied that the surveillance being sought to be authorised is likely to relate primarily to communications protected by privilege. (5) An authorisation may impose such conditions in respect of the surveillance authorised as the judge considers appropriate. (6) An authorisation shall be in writing and shall specify— (a) particulars of the surveillance device that is authorised to be used, (b) the person who, or the place or thing that, is to be the subject of the surveillance, (c) the name of the superior officer to whom it is issued, (d) the conditions (if any) subject to which the authorisation is issued, and (e) the date of expiry of the authorisation. (7) An authorisation may authorise the superior officer named in it, or any member of the Garda Síochána, any member of the Defence Forces or any officer of the Revenue Commissioners designated by that superior officer, accompanied by any other person whom he or she considers necessary, to enter, if necessary by the use of reasonable force, any place for the purposes of initiating or carrying out the authorised surveillance, and withdrawing the authorised surveillance device, without the consent of a person who owns or is in charge of the place. (8) An authorisation shall expire on the day fixed by the judge that he or she considers reasonable in the circumstances and that is not later than 3 months from the day on which it is issued. (9) Subject to any conditions imposed by the judge under subsection (5), an authorisation shall have effect both within the district court district to which the judge is assigned and in any other part of the State.	
What ongoing supervision is required for the use of this tool?	N/A	

Relevant items	Provisions	Sources used
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Undercover / covert operations		
Relevant documents (legal and non-legal) that define the functioning of the tool	As per A Human Rights Based Policing Approach in Ireland (2018) 'there is no legislation regulating the use of covert human intelligence sources (CHIS) commonly known as informers. Nor is there any law regulating the use or activities of undercover police', however the use of agents is mentioned in Public Statement by the Commissioner of An Garda Siochana on the Management and Use of Covert Human Intelligence Sources Undercover operations are covered by the term 'agents' in Public Statement by the Commissioner of An Garda Siochana on the Management and Use of Covert Human Intelligence Sources. 'The terms 'informant', 'informer' or 'source' are ones that are widely understood both within policing circles and the wider public. A more common term now in usage in many jurisdictions is 'Covert Human Intelligence Source'. This term or its acronym, CHIS, is also frequently used throughout this document and is sufficiently all embracing to incorporate three distinctly separate but related categories of person who provide information to police, i.e. – casual contacts, informants and agents.'	• A Human Rights Based Policing Approach in Ireland (2018) https://www.iccl.ie/wp-content/uploads/2018/09/Human-Rights-Based-Policing-in-Ireland.pdf • Public Statement by the Commissioner of An Garda Siochana on the Management and Use of Covert Human Intelligence Sources https://www.garda.ie/eN/About-us/publications/policy-documents/management-and-use-of-covert-human-intelligence-sources.pdf
How is the tool defined?	Public Statement by the Commissioner of An Garda Siochana on the Management and Use of Covert Human Intelligence Sources gives the following definition 'The terms 'informant', 'informer' or 'source' are ones that are widely understood both within policing circles and the wider public. A more common term now in usage in many jurisdictions is 'Covert Human Intelligence Source'. This term or its acronym, CHIS, is also frequently used throughout this document and is sufficiently all embracing to incorporate three distinctly separate but related categories of person who provide information to police, i.e. – casual contacts, informants and agents.'	• Public Statement by the Commissioner of An Garda Siochana on the Management and Use of Covert Human Intelligence Sources https://www.garda.ie/eN/About-us/publications/policy-documents/management-and-use-of-covert-human-intelligence-sources.pdf
For what types of crime can the tool be used?	Drugs, terrorism and other crimes. The Public Statement by the Commissioner of An Garda Siochana on the Management and Use of Covert Human Intelligence Sources discusses the below with relation to CHIS: 'An Garda Síochána seeks to tackle the consequence of crime, criminal and terrorist activity at several levels simultaneously; • To reduce, through intelligence led policing and international cooperation, the threat by groups involved in subversive and terrorist activity who seek to undermine democracy at national and international level • To reduce, in partnership with the community, the incidence and fear of organised, drug related and serious crime and of criminal behaviour • To ensure public safety by reducing the incidence of public disorder and antisocial behaviour with a view to making public places safe and enjoyable for all • To improve confidence in An Garda Síochána and in the criminal justice system by building a service that is deserving of the trust of the people of Ireland, by tackling those who intimidate witnesses, who promote the corruption of police officers, who exploit weaknesses in national and international jurisdictions and who seek to discover and disable advances in investigative techniques.'	• Public Statement by the Commissioner of An Garda Siochana on the Management and Use of Covert Human Intelligence Sources https://www.garda.ie/eN/About-us/publications/policy-documents/management-and-use-of-covert-human-intelligence-sources.pdf
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	In Public Statement by the Commissioner of An Garda Siochana on the Management and Use of Covert Human Intelligence Sources (CHIS) there is mention of a Code of Practice for the Management and Use of Covert Human Intelligence Sources which is available to all members of An Garda Síochána and is the basis of the professional standards required to maintain the confidence of the public and the courts in the continuing use of CHIS. However, the tool does not appear to be accessible to the public, so unable to find an answer to this question No mention of maximum term of imprisonment	• Public Statement by the Commissioner of An Garda Siochana on the Management and Use of Covert Human Intelligence Sources https://www.garda.ie/eN/About-us/publications/policy-documents/management-and-use-of-covert-human-intelligence-sources.pdf
What types of stakeholder are involved in the implementation of this tool?	In Public Statement by the Commissioner of An Garda Siochana on the Management and Use of Covert Human Intelligence Sources (CHIS) there is mention of a Code of Practice for the Management and Use of Covert Human Intelligence Sources which is available to all members of An Garda Síochána and is the basis of the professional standards required to maintain the	• Public Statement by the Commissioner of An Garda Siochana on the Management and Use of Covert Human Intelligence Sources https://www.garda.ie/eN/About-us/publications/policy-documents/management-and-use-of-covert-human-intelligence-sources.pdf

Relevant items	Provisions	Sources used
	confidence of the public and the courts in the continuing use of CHIS. However, the tool does not appear to be accessible to the public, so unable to find an answer to this question	
Which LEAs can use this tool?	In Public Statement by the Commissioner of An Garda Síochána on the Management and Use of Covert Human Intelligence Sources (CHIS) there is mention of a Code of Practice for the Management and Use of Covert Human Intelligence Sources which is available to all members of An Garda Síochána and is the basis of the professional standards required to maintain the confidence of the public and the courts in the continuing use of CHIS. However, the tool does not appear to be accessible to the public, so unable to find an answer to this question. However Public Statement by the Commissioner of An Garda Síochána on the Management and Use of Covert Human Intelligence Sources mentions that CHIS should be used by experienced personnel: 'The Mission Statement of An Garda Síochána for the management of CHIS is; "the assessment, recruitment and use of Covert Human Intelligence Sources (CHIS) is a skilled Police function, demanding the highest standards of integrity and shall be conducted by experienced personnel, working in a secure environment to the clear requirements of an informed and supportive management".'	- Public Statement by the Commissioner of An Garda Síochána - on the Management and Use of Covert Human Intelligence Sources https://www.garda.ie/eN/About-us/publications/policy-documents/management-and-use-of-covert-human-intelligence-sources.pdf
What are the rules to be followed for the implementation of this tool?	In Public Statement by the Commissioner of An Garda Síochána on the Management and Use of Covert Human Intelligence Sources (CHIS) there is mention of a Code of Practice for the Management and Use of Covert Human Intelligence Sources which is available to all members of An Garda Síochána and is the basis of the professional standards required to maintain the confidence of the public and the courts in the continuing use of CHIS. However, the tool does not appear to be accessible to the public, so unable to find an answer to this question	- Public Statement by the Commissioner of An Garda Síochána - on the Management and Use of Covert Human Intelligence Sources https://www.garda.ie/eN/About-us/publications/policy-documents/management-and-use-of-covert-human-intelligence-sources.pdf
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Public Statement by the Commissioner of An Garda Síochána on the Management and Use of Covert Human Intelligence Sources (CHIS) states: 'An Garda Síochána has a duty to protect the identity of a CHIS and as such we have a duty of care to these individuals. This duty will necessitate that a risk assessment is conducted in respect of each CHIS. The risk assessment procedures governed by Public Statement by the Commissioner of An Garda Síochána on the Management and Use of Covert Human Intelligence Sources Mission Statement: To achieve the highest level of Personal Protection, Community Commitment and State Security the Code of Practice help manage the risks to CHIS, members of An Garda Síochána, and third parties'. The Code of Practice does not appear to be available to the public so cannot find information on the details here	- Public Statement by the Commissioner of An Garda Síochána - on the Management and Use of Covert Human Intelligence Sources https://www.garda.ie/eN/About-us/publications/policy-documents/management-and-use-of-covert-human-intelligence-sources.pdf
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	In Public Statement by the Commissioner of An Garda Síochána on the Management and Use of Covert Human Intelligence Sources (CHIS) there is mention of a Code of Practice for the Management and Use of Covert Human Intelligence Sources which is available to all members of An Garda Síochána and is the basis of the professional standards required to maintain the confidence of the public and the courts in the continuing use of CHIS. However, the tool does not appear to be accessible to the public, so unable to find an answer to this question	- Public Statement by the Commissioner of An Garda Síochána - on the Management and Use of Covert Human Intelligence Sources https://www.garda.ie/eN/About-us/publications/policy-documents/management-and-use-of-covert-human-intelligence-sources.pdf
What ongoing supervision is required for the use of this tool?	In Public Statement by the Commissioner of An Garda Síochána on the Management and Use of Covert Human Intelligence Sources (CHIS) there is mention of a Code of Practice for the Management and Use of Covert Human Intelligence Sources which is available to all members of An Garda Síochána and is the basis of the professional standards required to maintain the confidence of the public and the courts in the continuing use of CHIS. However, the tool does not appear to be accessible to the public, so unable to find an answer to this question	- Public Statement by the Commissioner of An Garda Síochána - on the Management and Use of Covert Human Intelligence Sources https://www.garda.ie/eN/About-us/publications/policy-documents/management-and-use-of-covert-human-intelligence-sources.pdf
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	Informants or Covert Human Intelligence Services are used as detailed in Public Statement by the Commissioner of An Garda Síochána on the Management and Use of Covert Human Intelligence Sources, however as per A Human Rights Based Policing Approach in Ireland (2018) 'there is no legislation regulating the use of covert human intelligence sources (CHIS) commonly known as informers.'	- Public Statement by the Commissioner of An Garda Síochána - on the Management and Use of Covert Human Intelligence Sources https://www.garda.ie/eN/About-us/publications/policy-documents/management-and-use-of-covert-human-intelligence-sources.pdf - A Human Rights Based Policing Approach in Ireland (2018): https://www.iccl.ie/wp-content/uploads/2018/09/Human-Rights-Based-Policing-in-Ireland.pdf
Specific range of application of the tool	There is no national legislation which details this however, the Public Statement by the Commissioner of An Garda Síochána on the Management and Use of Covert Human Intelligence Sources mentions CHIS 'is sufficiently all embracing to incorporate three distinctly separate but related categories of person who provide information to police, i.e. – casual contacts, informants and agents.'	- Public Statement by the Commissioner of An Garda Síochána - on the Management and Use of Covert Human Intelligence Sources https://www.garda.ie/eN/About-us/publications/policy-documents/management-and-use-of-covert-human-intelligence-sources.pdf

Relevant items	Provisions	Sources used
How is the tool defined?	Public Statement by the Commissioner of An Garda Síochána on the Management and Use of Covert Human Intelligence Sources says: 'The terms 'informant', 'informer' or 'source' are ones that are widely understood both within policing circles and the wider public. A more common term now in usage in many jurisdictions is 'Covert Human Intelligence Source'. This term or its acronym, CHIS, is also frequently used throughout this document and is sufficiently all embracing to incorporate three distinctly separate but related categories of person who provide information to police, i.e. – casual contacts, informants and agents.'	- Public Statement by the Commissioner of An Garda Síochána - on the Management and Use of Covert Human Intelligence Sources https://www.garda.ie/eN/About-us/publications/policy-documents/management-and-use-of-covert-human-intelligence-sources.pdf
For what types of crime can the tool be used?	Drugs, terrorism and other crimes. The Public Statement by the Commissioner of An Garda Síochána on the Management and Use of Covert Human Intelligence Sources discusses the below with relation to CHIS: 'An Garda Síochána seeks to tackle the consequence of crime, criminal and terrorist activity at several levels simultaneously; - To reduce, through intelligence led policing and international cooperation, the threat by groups involved in subversive and terrorist activity who seek to undermine democracy at national and international level - To reduce, in partnership with the community, the incidence and fear of organised, drug related and serious crime and of criminal behaviour - To ensure public safety by reducing the incidence of public disorder and antisocial behaviour with a view to making public places safe and enjoyable for all - To improve confidence in An Garda Síochána and in the criminal justice system by building a service that is deserving of the trust of the people of Ireland, by tackling those who intimidate witnesses, who promote the corruption of police officers, who exploit weaknesses in national and international jurisdictions and who seek to discover and disable advances in investigative techniques.'	- Public Statement by the Commissioner of An Garda Síochána - on the Management and Use of Covert Human Intelligence Sources https://www.garda.ie/eN/About-us/publications/policy-documents/management-and-use-of-covert-human-intelligence-sources.pdf
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	In Public Statement by the Commissioner of An Garda Síochána on the Management and Use of Covert Human Intelligence Sources (CHIS) there is mention of a Code of Practice for the Management and Use of Covert Human Intelligence Sources which is available to all members of An Garda Síochána and is the basis of the professional standards required to maintain the confidence of the public and the courts in the continuing use of CHIS. However, the tool does not appear to be accessible to the public, so unable to find an answer to this question No mention of maximum term of imprisonment	- Public Statement by the Commissioner of An Garda Síochána - on the Management and Use of Covert Human Intelligence Sources https://www.garda.ie/eN/About-us/publications/policy-documents/management-and-use-of-covert-human-intelligence-sources.pdf
What types of stakeholder are involved in the implementation of this tool?	In Public Statement by the Commissioner of An Garda Síochána on the Management and Use of Covert Human Intelligence Sources (CHIS) there is mention of a Code of Practice for the Management and Use of Covert Human Intelligence Sources which is available to all members of An Garda Síochána and is the basis of the professional standards required to maintain the confidence of the public and the courts in the continuing use of CHIS. However, the tool does not appear to be accessible to the public, so unable to find an answer to this question	- Public Statement by the Commissioner of An Garda Síochána - on the Management and Use of Covert Human Intelligence Sources https://www.garda.ie/eN/About-us/publications/policy-documents/management-and-use-of-covert-human-intelligence-sources.pdf
Which LEAs can use this tool?	In Public Statement by the Commissioner of An Garda Síochána on the Management and Use of Covert Human Intelligence Sources (CHIS) there is mention of a Code of Practice for the Management and Use of Covert Human Intelligence Sources which is available to all members of An Garda Síochána and is the basis of the professional standards required to maintain the confidence of the public and the courts in the continuing use of CHIS. However, the tool does not appear to be accessible to the public, so unable to find an answer to this question	- Public Statement by the Commissioner of An Garda Síochána - on the Management and Use of Covert Human Intelligence Sources https://www.garda.ie/eN/About-us/publications/policy-documents/management-and-use-of-covert-human-intelligence-sources.pdf
What are the rules to be followed for the implementation of this tool?	In Public Statement by the Commissioner of An Garda Síochána on the Management and Use of Covert Human Intelligence Sources (CHIS) there is mention of a Code of Practice for the Management and Use of Covert Human Intelligence Sources which is available to all members of An Garda Síochána and is the basis of the professional standards required to maintain the confidence of the public and the courts in the continuing use of CHIS. However, the tool does not appear to be accessible to the public, so unable to find an answer to this question	- Public Statement by the Commissioner of An Garda Síochána - on the Management and Use of Covert Human Intelligence Sources https://www.garda.ie/eN/About-us/publications/policy-documents/management-and-use-of-covert-human-intelligence-sources.pdf
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Public Statement by the Commissioner of An Garda Síochána on the Management and Use of Covert Human Intelligence Sources (CHIS) states: 'An Garda Síochána has a duty to protect the identity of a CHIS and as such we have a duty of care to these individuals. This duty will necessitate that a risk assessment is conducted in respect of each CHIS. The risk assessment procedures governed by Public Statement by the Commissioner of An Garda Síochána on the Management and Use of Covert Human Intelligence Sources Mission Statement: To achieve the highest level of Personal Protection, Community Commitment and State Security the Code of Practice help manage the risks to CHIS, members of An Garda Síochána, and third parties'. The Code of Practice does not appear to be available to the public so cannot find information on the details here	- Public Statement by the Commissioner of An Garda Síochána - on the Management and Use of Covert Human Intelligence Sources https://www.garda.ie/eN/About-us/publications/policy-documents/management-and-use-of-covert-human-intelligence-sources.pdf
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	In Public Statement by the Commissioner of An Garda Síochána on the Management and Use of Covert Human Intelligence Sources (CHIS) there is mention of a Code of Practice for the Management and Use of Covert Human Intelligence Sources which is available to all members of	Public Statement by the Commissioner of An Garda Síochána

Relevant items	Provisions	Sources used
	An Garda Síochána and is the basis of the professional standards required to maintain the confidence of the public and the courts in the continuing use of CHIS. However, the tool does not appear to be accessible to the public, so unable to find an answer to this question	on the Management and Use of Covert Human Intelligence Sources https://www.garda.ie/eN/About-us/publications/policy-documents/management-and-use-of-covert-human-intelligence-sources.pdf
What ongoing supervision is required for the use of this tool?	In Public Statement by the Commissioner of An Garda Síochána on the Management and Use of Covert Human Intelligence Sources (CHIS) there is mention of a Code of Practice for the Management and Use of Covert Human Intelligence Sources which is available to all members of An Garda Síochána and is the basis of the professional standards required to maintain the confidence of the public and the courts in the continuing use of CHIS. However, the tool does not appear to be accessible to the public, so unable to find an answer to this question	- Public Statement by the Commissioner of An Garda Síochána - on the Management and Use of Covert Human Intelligence Sources https://www.garda.ie/eN/About-us/publications/policy-documents/management-and-use-of-covert-human-intelligence-sources.pdf
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	

Source: Author's own elaboration

Italy

Table 33 – Overview of national rules on investigative tools - Italy

Relevant items	Provisions	Sources used
Controlled Delivery		
Relevant documents (legal and non-legal) that define the functioning of the tool	Law of 16 March 2006, no. 146 (Article 9), Dpr n. 309/1990, Legislative Decree 5 April 2017, no 52 (art. 16)	https://www.gazzettaufficiale.it/eli/id/2017/04/27/17G00065/sq#:~:text=Il%20presente%20decreto%20reca%20disposizioni,Bruxelles%20il%2029%20maggio%202000.https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2006-04-11&atto.codiceRedazionale=006G0168&elenco30giorni=falsehttps://www.gazzettaufficiale.it/eli/id/1990/10/31/090G0363/sq
How is the tool defined?	not defined. The tool is an exemption from criminal liability for the omission committed during the operation	Legislative Decree 5 April 2017, no 52 (art. 16) https://www.gazzettaufficiale.it/eli/id/2017/04/27/17G00065/sq#:~:text=Il%20presente%20decreto%20reca%20disposizioni,Bruxelles%20il%2029%20maggio%202000.
For what types of crime can the tool be used?	Drugs, Financial crimes, Environmental crime, Trafficking of firearms, Illegal immigration, Terrorism plus: Crimes against the Public Administration, forgery of money and means of payment, counterfeiting, extortion, usury, kidnapping for ransom, crimes against individual personality and freedom, exploitation of prostitution.	Law of 16 March 2006, no. 146 (Article 9) https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2006-04-11&atto.codiceRedazionale=006G0168&tipoDettaglio=multivigenza&qId=&tabID=0.5617783247471355&title=Atto%20multivigente&bloccoAggiornamentoBreadCrum b=true
Does national law allow this tool to be used in cross border cases?	cross border criminal investigations	
What thresholds must be passed for the use of this tool?	no reference to imprisonment.	
What types of stakeholder are involved in the implementation of this tool?	Police, Carabinieri, Guardia di Finanza officers as well as officers belonging to the special structures of the Antimafia Investigative Direction (DIA- Direzione Investigativa Antimafia), Police and Carabinieri belonging to Antiterrorism department, Finance Police (Guardia di Finanza) competent to avoid financing of terrorism. Public prosecutor, judicial authority. The use of the tool is allowed by the top bodies of the law enforcement agency, or by its delegate in charge. Before the use of the tool the competent Public Prosecutor shall be informed as well as during the use of the tool. If police has to omit or delay their action, the competent Public Prosecutor shall be immediately informed. The Public Prosecutor leads the operation and informs the judicial competent authority of the place where the operation shall conclude or transit. The Public Prosecutor shall transmit relevant documents to the Chief Public Prosecutor at the Court of Appeal (Procuratore Generale della Corte d'Appello). In case of crimes related to mafia, the Anti-mafia Chief Prosecutor shall be informed.	Law of 16 March 2006, no. 146 (Article 9, 1, a and b) https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2006-04-11&atto.codiceRedazionale=006G0168&tipoDettaglio=multivigenza&qId=&tabID=0.5617783247471355&title=Atto%20multivigente&bloccoAggiornamentoBreadCrum b=true
Which LEAs can use this tool?	Police, Carabinieri, Guardia di Finanza officers as well as officers belonging to the special structures of the Antimafia Investigative Direction (DIA- Direzione Investigativa Antimafia), Police and Carabinieri belonging to Antiterrorism department, Finance Police (Guardia di Finanza) competent to avoid financing of terrorism	Law of 16 March 2006, no. 146 (Article 9, 3,4, 6, 7, 8) https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2006-04-11&atto.codiceRedazionale=006G0168&tipoDettaglio=multivigenza&qId=&tabID=0

Relevant items	Provisions	Sources used
		.5617783247471355&title=Atto%20multivigente&bloccoAggiornamentoBreadCrum b=true
What are the rules to be followed for the implementation of this tool?	The tool can be used during police operations to find evidence relating to crimes listed above or to find and arrest those who have committed the crimes. 1)The use of the tool is allowed by the top bodies of the law enforcement agency, or by its delegate in charge, at least, at the provincial level. In case of crimes related to immigration (Legislative Decree 286/1998) the authorisation to use the tool shall be in agreement with the Central Directorate of Immigration and Border Police. Before the use of the tool the competent Public Prosecutor shall be informed as well as during the use of the tool. 2) If, in order to find or arrest those who committed a crime police has to omit or delay their action, the competent Public Prosecutor shall be immediately informed. If the information was oral, a detailed report shall be sent to the Public Prosecutor within 48 hours. The Public Prosecutor leads the operation and informs the judicial competent authority of the place where the operation shall conclude or transit. The Public Prosecutor shall transmit relevant documents to the Chief Public Prosecutor at the Court of Appeal (Procuratore Generale della Corte d'Appello). In case of crimes related to mafia, the Anti-mafia Chief Prosecutor shall be informed.	Law of 16 March 2006, no. 146 (Article 9, 3,4, 6, 7, 8) https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2006-04-11&atto.codiceRedazionale=006G0168&tipoDettaglio=multivigenza&qId=&tabID=0 .5617783247471355&title=Atto%20multivigente&bloccoAggiornamentoBreadCrum b=true
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	during a hot pursuit police shall not instigate someone to commit a crime; police shall only search for evidence of the crime	- Cass 3, Sentenza n. 37805 del 09/05/2013 - https://archiviodpc.dirittopenaleuomo.org/d/6527-lagente-sotto-copertura-per-i-reati-di-corruzione-nel-quadro-delle-tecniche-speciali-di-investigazi#_ftn17
What authorisation is needed for the use of this tool?	1) The use of the tool is allowed by the top bodies of the law enforcement agency, or by its delegate in charge, at least, at the provincial level. In case of crimes related to immigration (Legislative Decree 286/1998) the authorisation to use the tool shall be in agreement with the Central Directorate of Immigration and Border Police. Before the use of the tool the competent Public Prosecutor shall be informed as well as during the use of the tool. 2) If, in order to find or arrest those who committed a crime police has to omit or delay their action, the competent Public Prosecutor shall be immediately informed. If the information was oral, a detailed report shall be sent to the Public Prosecutor within 48 hours. The Public Prosecutor leads the operation and informs the judicial competent authority of the place where the operation shall conclude or transit. The Public Prosecutor shall transmit relevant documents to the Chief Public Prosecutor at the Court of Appeal (Procuratore Generale della Corte d'Appello). In case of crimes related to mafia, the Anti-mafia Chief Prosecutor shall be informed	Law of 16 March 2006, no. 146 (Article 9, 6, 7 and 8) https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2006-04-11&atto.codiceRedazionale=006G0168&elenco30giorni=false
What ongoing supervision is required for the use of this tool?	Supervision from Public Prosecutor and, If, in order to find or arrest those who committed a crime police has to omit or delay their action, Chief Public Prosecutor at the Court of Appeal and, if the crime is related to mafia, Anti-mafia Chief Prosecutor	Law of 16 March 2006, no. 146 (Article 9, 3,4, 6, 7, 8) https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2006-04-11&atto.codiceRedazionale=006G0168&tipoDettaglio=multivigenza&qId=&tabID=0 .5617783247471355&title=Atto%20multivigente&bloccoAggiornamentoBreadCrum b=true
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Data available on the number of times this tool has been used for SOC cases	N/A	
Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	19 June 1990 Convention implementing the Schengen Agreement (CISA) - Art. 41 and Convention of 18.12.1997 on mutual assistance and cooperation between customs administrations (Naples II Convention) art. 20 ACCORDO SULLA COOPERAZIONE DI POLIZIA E DOGANALE TRA IL GOVERNO DELLA REPUBBLICA ITALIANA E IL CONSIGLIO FEDERALE SVIZZERO	19 June 1990 Convention implementing the Schengen Agreement (CISA) - Art. 41 and Convention of 18.12.1997 on mutual assistance and cooperation between customs administrations (Naples II Convention) art. 20 - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/uri=CELEX:31998F0123(01) - http://www.governo.it/sites/governo.it/files/accordo_firmato.pdf - https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922(02):EN:HTML
How is the tool defined?	Officers of the customs administration of one of the Member States pursuing in their country, an individual observed in the act of committing one of the infringements referred to in Article 19(2) which could give rise to extradition, or participating in such an infringement, shall be authorised to continue pursuit in the territory of another Member State without prior authorisation where, given the particular urgency of the situation, it was not possible to notify the competent authorities of the other Member State prior to entry into that territory or where these authorities have been unable to reach the scene in time to take the pursuit.	19 June 1990 Convention implementing the Schengen Agreement (CISA) - Art. 41 and Convention of 18.12.1997 on mutual assistance and cooperation between customs administrations (Naples II Convention) art. 20 - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/uri=CELEX:31998F0123(01) - https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922(02):EN:HTML
For what types of crime can the tool be used?	Pursuant to Art. 19 of the Naples II Convention the tool can be used for the following crimes: illicit traffic of drugs, weapons, cultural goods, toxic waste nuclear material and materials for the manufacture of atomic, biological and/or chemical weapons; precursor substance for the manufacture of drugs and psychotropic substances; illegal cross-border commercial trade in	19 June 1990 Convention implementing the Schengen Agreement (CISA) - Art. 41 and Convention of 18.12.1997 on mutual assistance and cooperation between customs administrations (Naples II Convention) art. 20 - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/uri=CELEX:31998F0123(01)

Relevant items	Provisions	Sources used
	taxable goods to evade tax or to obtain unauthorised State payments in connection with the import or export of goods; any other trade in goods prohibited by Community or national rules.	https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922(02):EN:HTML
Does national law allow this tool to be used in cross border cases?	cross border criminal investigations	
What thresholds must be passed for the use of this tool?	Pursuant to art. 19 (2) of the Naples II Convention there must be serious grounds for believing that the subject is involved in one of the following infringements: illicit traffic of drugs, weapons, cultural goods, toxic waste nuclear material and materials for the manufacture of atomic, biological and/or chemical weapons; precursor substance for the manufacture of drugs and psychotropic substances; illegal cross-border commercial trade in taxable goods to evade tax or to obtain unauthorised State payments in connection with the import or export of goods; any other trade in goods prohibited by Community or national rules. Furthermore, requirements of flagrancy and near-flagrancy of art. 382 of Italian Criminal Procedure Code must be respected. Pursuant to Art. 1 Law No. 388 of 1993 such tool may be used only in occasion of one of the following offences: murder, rape, arson, counterfeit currency, aggravated theft and receiving stolen property, extortion, kidnapping and hostage taking, trafficking in persons, unlawful trafficking in narcotic drugs and psychotropic substances, infringement of weapons and explosives regulations, destruction by means of explosives, unlawful transportation of toxic and harmful waste.	Law No. 388 of 1993 Art. 1 https://www.esteri.it/mae/normative/normativa_consolare/visti/schengen.pdf
What types of stakeholder are involved in the implementation of this tool?	Public Prosecutor and LEA agencies listed above	19 June 1990 Convention implementing the Schengen Agreement (CISA) - Art. 41 and Convention of 18.12.1997 on mutual assistance and cooperation between customs administrations (Naples II Convention) art. 20 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/uri=CELEX:31998F0123(01) https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922(02):EN:HTML
Which LEAs can use this tool?	Custom administration authorities, Police, Carabinieri, Guardia di Finanza officers as well as officers belonging to the special structures of the Antimafia Investigative Direction (DIA-Direzione Investigativa Antimafia), Police and Carabinieri belonging to Antiterrorism department, Finance Police (Guardia di Finanza) competent to avoid financing of terrorism	19 June 1990 Convention implementing the Schengen Agreement (CISA) - Art. 41 and Convention of 18.12.1997 on mutual assistance and cooperation between customs administrations (Naples II Convention) art. 20 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/uri=CELEX:31998F0123(01) https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922(02):EN:HTML
What are the rules to be followed for the implementation of this tool?	The tool must comply with the rules of: - Flagrancy or near flagrancy of a crime - Notification to the competent authorities - Crimes listed above	19 June 1990 Convention implementing the Schengen Agreement (CISA) - Art. 41 and Convention of 18.12.1997 on mutual assistance and cooperation between customs administrations (Naples II Convention) art. 20 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/uri=CELEX:31998F0123(01) https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922(02):EN:HTML
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	in the interest of individuals, the tool shall be used only in case of Flagrancy or near-flagrancy of a crime, pursuant to art. 382 of the Italian Criminal Procedure Code, when the crime the pursuit starts in the Italian territory.	- Art. 382 of the Italian Criminal Procedure Code https://www.gazzettaufficiale.it/anteprima/codici/codiceProceduraPenale
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	During a hot pursuit the Judicial Police is authorised to continue pursuit in the territory of another Member State without prior authorisation where, given the particular urgency of the situation, it was not possible to notify the competent authorities. In any case the Judicial Police shall notify subsequently such fact to the competent Public Prosecutor's office.	19 June 1990 Convention implementing the Schengen Agreement (CISA) - Art. 41 and Convention of 18.12.1997 on mutual assistance and cooperation between customs administrations (Naples II Convention) art. 20 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/uri=CELEX:31998F0123(01) https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:42000A0922(02):EN:HTML
What ongoing supervision is required for the use of this tool?	Pursuant to article 4 (3) of law No. 217 of 30/12/2008, in accordance with articles 20 of the "Naples II Convention", after obtainment of the authorisation from the competent Judicial Authority of the MS in which the activity is taking place, unless such Authority revokes the authorisation the operations, may proceed and in any case in observance of conditions set in article and 21(2).	- Law No. 217 of 30/12/2008 article 4 (3) https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1983;217;
Is there any national case law relating to the use of this tool in cross-border crime cases?	Pursuant to Ginevra's Convention, the Italian police can pursuit a boat in international water if said boat has no flag. The case-law makes reference to the Italian jurisdiction in case of maritime cross-border hot pursuit	Cassazione penale , sez. IV , 08/03/2018 , n. 14709
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	no data available	
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	Law 11.01.2018, no. 6 Law 15.03.1991, no. 82 Law Decree 15.01.1991, no. 8	https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2018-01-11;6 https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=1991-03-16&atto.codiceRedazionale=091G0128&atto.articolo.numero=0&qId=11b04054-

Relevant items	Provisions	Sources used
		c2e6-4180-a002-300f35bde793&tabID=0.7261548165615357&title=lbl.dettaglioAtto https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:1991;8
How is the tool defined?	Witness protection is a Special protection measures for witnesses; it may consist of protection measures, economic support measures, social and work reintegration	
For what types of crime can the tool be used?	terrorism, criminal association, illegal immigration, counterfeit, environmental crimes.	
Does national law allow this tool to be used in cross border cases?	cross border criminal investigations	
What thresholds must be passed for the use of this tool?		
What types of stakeholder are involved in the implementation of this tool?	central committee decides if the protection shall be granted; Public prosecutor asks for witness protection; District Anti-Mafia Directorate asks for witness protection (if related to mafia); Chief of police asks for witness protection	
Which LEAs can use this tool?	Chief of police may ask for witness protection	
What are the rules to be followed for the implementation of this tool?	in order to be protected the witness shall collaborate, be reliable, grant information new, relevant. protection shall be granted when the witness faces a serious and immediate danger. Protection shall be granted to whom related to the witness are in danger cause the witness collaboration.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	close family and close people may use protection. Protection may consist even of economic support, social and work reintegration	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	central committee	
What ongoing supervision is required for the use of this tool?	central committee	
Is there any national case law relating to the use of this tool in cross-border crime cases?	1. the case law affirms that witness protection shall be granted to close family 2. extradition of a witness: one country shall verify if the other country can adequately protect the witness before accepting the extradition	- non crossborder: T.A.R. Roma, (Lazio) sez. I, 03/05/2017, n.5141 - Cassazione penale sez. VI, 20/01/2015, n.6488
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Surveillance		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Procedure Code, Title III, Chapter IV, articles 266 and following. Law No. 161 of 30 December 2019	Criminal Procedure Code, Title III, Chapter IV, articles 266 and following https://www.gazzettaufficiale.it/anteprema/codici/codiceProceduraPenale Law No. 161 of 30 December 2019 https://www.gazzettaufficiale.it/eli/id/2019/12/31/19G00169/sg
Specific range of application of the tool	No speck surveillance tools are mentioned within the Italian Criminal Procedure Code. Nonetheless, all tools falls within the definition of "means of searching for evidence" listed in art 266 and subs. The law only makes reference to: - Telephone communication and conversations; - Other means of telecommunication; - Informatic data surveillance under art. 266-bis; - Wiretapping under art. 267; - Cyber captors under Law No. 161 of 30 December 2019.	Criminal Procedure Code, Title III, Chapter IV, articles 266 and following https://www.gazzettaufficiale.it/anteprema/codici/codiceProceduraPenale Law No. 161 of 30 December 2019 https://www.gazzettaufficiale.it/eli/id/2019/12/31/19G00169/sg
How is the tool defined?	N/A	N/A
For what types of crime can the tool be used?	By means of art. 266 of the Criminal Procedure Code, they are used in preliminary investigations concerning crimes related to organised crime, drug traffic and terrorism; non-negligent offences for which the punishment is life imprisonment or imprisonment for a maximum of more than five years; offences against the public administration for which the punishment is life imprisonment or imprisonment for a maximum period of not less than five years; offences involving narcotic drugs or psychotropic substances; offences related to weapons and explosive substances; offences of smuggling; crimes of insult, threat, usury, abusive financial activity, abuse of privileged information, market manipulation, harassment or disturbance of persons by means of telephone.	Criminal Procedure Code, Title III, Chapter IV, articles 266 and following https://www.gazzettaufficiale.it/anteprema/codici/codiceProceduraPenale Law No. 161 of 30 December 2019 https://www.gazzettaufficiale.it/eli/id/2019/12/31/19G00169/sg
Does national law allow this tool to be used in cross border cases?	cross border criminal investigations	

Relevant items	Provisions	Sources used
What thresholds must be passed for the use of this tool?	By means of art. 266 of the Criminal Procedure Code, they are used in preliminary investigations concerning crimes related to organised crime, drug traffic and terrorism; non-negligent offences for which the punishment is life imprisonment or imprisonment for a maximum of more than five years; offences against the public administration for which the punishment is life imprisonment or imprisonment for a maximum period of not less than five years; offences involving narcotic drugs or psychotropic substances; offences related to weapons and explosive substances; offences of smuggling; crimes of insult, threat, usury, abusive financial activity, abuse of privileged information, market manipulation, harassment or disturbance of persons by means of telephone.	Criminal Procedure Code, Title III, Chapter IV, articles 266 and following https://www.gazzettaufficiale.it/anteprema/codici/codiceProceduraPenale Law No. 161 of 30 December 2019 https://www.gazzettaufficiale.it/eli/id/2019/12/31/19G00169/sg
What types of stakeholder are involved in the implementation of this tool?	Police, Carabinieri, Guardia di Finanza officers as well as officers belonging to the special structures of the Antimafia Investigative Direction (DIA- Direzione Investigativa Antimafia), Police and Carabinieri belonging to Antiterrorism department, Finance Police (Guardia di Finanza) competent to avoid financing of terrorism	Criminal Procedure Code, Title III, Chapter IV, articles 266 and following https://www.gazzettaufficiale.it/anteprema/codici/codiceProceduraPenale Law No. 161 of 30 December 2019 https://www.gazzettaufficiale.it/eli/id/2019/12/31/19G00169/sg
Which LEAs can use this tool?	Concerning wiretapping under art. 267 of the Italian Criminal Procedure Code, the Public Prosecutor shall apply to the judge in charge of preliminary investigations for authorisation to order the operations set forth in article 266. The authorisation shall be given by means of a motivated decree when there are serious indications of a crime and the wiretapping is absolutely essential for the continuation of the investigation. The decree authorizing wiretapping between persons present through the insertion of a computer interceptor on a portable electronic device shall indicate the reasons that make this modality necessary for the conduct of investigations; as well as, if proceedings are brought for offences other than those referred to in article 51, paragraphs 3-bis and 3-quater, and offences committed by public officials or public service officers against the public administration for which a penalty of imprisonment of not less than a maximum of five years is envisaged, determined in accordance with article 4, the places and time, even indirectly determined, in relation to which activation of the microphone is permitted.	Criminal Procedure Code, Title III, Chapter IV, articles 266 and following https://www.gazzettaufficiale.it/anteprema/codici/codiceProceduraPenale Law No. 161 of 30 December 2019 https://www.gazzettaufficiale.it/eli/id/2019/12/31/19G00169/sg
What are the rules to be followed for the implementation of this tool?	It is always forbidden to publish, even partially, the contents of wiretaps that have not been acquired pursuant to articles 268 and 415-bis of the Italian Criminal Procedure Code.	Criminal Procedure Code, Title III, Chapter IV, articles 266 and following https://www.gazzettaufficiale.it/anteprema/codici/codiceProceduraPenale Law No. 161 of 30 December 2019 https://www.gazzettaufficiale.it/eli/id/2019/12/31/19G00169/sg
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	It is always forbidden to publish, even partially, the contents of wiretaps that have not been acquired pursuant to articles 268 and 415-bis of the Italian Criminal Procedure Code.	Criminal Procedure Code, Title III, Chapter IV, articles 266 and following https://www.gazzettaufficiale.it/anteprema/codici/codiceProceduraPenale Law No. 161 of 30 December 2019 https://www.gazzettaufficiale.it/eli/id/2019/12/31/19G00169/sg
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Public Prosecutor and Judge under art. 267.	
What ongoing supervision is required for the use of this tool?	Public Prosecutor and Judge under art. 267.	
Is there any national case law relating to the use of this tool in cross-border crime cases?	1. The interception of communications between persons present, carried out in part even abroad by means of a computer pick-up device installed in the national territory on mobile users connected to Italian telephone operators, does not require the activation of an international rogatory. 2. the acquisition of incoming and outgoing e-mail messages relating to a mailbox managed by a foreign provider through the routing procedure is legitimate	1. Cassazione penale sez. II, 22/07/2020, n.29362 2. Cassazione penale sez. IV, 28/06/2016, n.40903
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Undercover / covert operations		
Relevant documents (legal and non-legal) that define the functioning of the tool	Law of 16 March 2006, no. 146 (Article 9), Dpr n. 309/1990, Legislative Decree 5 April 2017, no 52 (art. 16)	Legislative Decree 5 April 2017, no 52 (art. 16) https://www.gazzettaufficiale.it/eli/id/2017/04/27/17G00065/sg#:~:text=Il%20pr%20presente%20decreto%20reca%20disposizioni,Bruxelles%20il%2029%20maggio%202000. Law of 16 March 2006, no. 146 (Article 9) https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2006-04-11&atto.codiceRedazionale=006G0168&tipoDettaglio=multivigenza&qId=&tabID=0.5617783247471355&title=Atto%20multivigente&bloccoAggiornamentoBreadcrumb=true
How is the tool defined?	The tool is an exemption from criminal liability for the crimes/omission committed during the operation	Legislative Decree 5 April 2017, no 52 (art. 16) https://www.gazzettaufficiale.it/eli/id/2017/04/27/17G00065/sg#:~:text=Il%20pr%20presente%20decreto%20reca%20disposizioni,Bruxelles%20il%2029%20maggio%202000. Law of 16 March 2006, no. 146 (Article 9) https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2006-04-11&atto.codiceRedazionale=006G0168&tipoDettaglio=multivigenza&qId=&tabID=0.5617783247471355&title=Atto%20multivigente&bloccoAggiornamentoBreadcrumb=true

Relevant items	Provisions	Sources used
		=2006-04-11&atto.codiceRedazionale=006G0168&tipoDettaglio=multivigenza&qId=&tabID=0.5617783247471355&title=Atto%20multivigente&bloccoAggiornamentoBreadCrum b=true
For what types of crime can the tool be used?	Drugs, forgery of money and means of payment, counterfeiting, extortion, kidnapping for ransom, usury, money laundering, use of money deriving from a crime, crimes against individual personality and freedom, offences connected to the use of weapons, ammunitions, explosive materials, Illegal immigration, environmental crimes, exploitation of prostitution, terrorism.	Law of 16 March 2006, no. 146 (Article 9) https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2006-04-11&atto.codiceRedazionale=006G0168&tipoDettaglio=multivigenza&qId=&tabID=0.5617783247471355&title=Atto%20multivigente&bloccoAggiornamentoBreadCrum b=true
Does national law allow this tool to be used in cross border cases?	cross border criminal investigations	Law of 16 March 2006, no. 146 (Article 9, sub 1, a and b) https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2006-04-11&atto.codiceRedazionale=006G0168&tipoDettaglio=multivigenza&qId=&tabID=0.5617783247471355&title=Atto%20multivigente&bloccoAggiornamentoBreadCrum b=true
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	"Police, Carabinieri, Guardia di Finanza officers as well as officers belonging to the special structures of the Antimafia Investigative Direction (DIA- Direzione Investigativa Antimafia), Police and Carabinieri belonging to Antiterrorism department, Finance Police (Guardia di Finanza) competent to avoid financing of terrorism. Public prosecutor, judicial authority.	
Which LEAs can use this tool?	The use of the tool is allowed by the top bodies of the law enforcement agency, or by its delegate in charge. Before the use of the tool the competent Public Prosecutor shall be informed as well as during the use of the tool. If police has to omit or delay their action, the competent Public Prosecutor shall be immediately informed. The Public Prosecutor leads the operation and informs the judicial competent authority of the place where the operation shall conclude or transit. The Public Prosecutor shall transmit relevant documents to the Chief Public Prosecutor at the Court of Appeal (Procuratore Generale della Corte d'Appello). In case of crimes related to mafia, the Anti-mafia Chief Prosecutor shall be informed."	Law of 16 March 2006, no. 146 (Article 9, sub 1, a and b) https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2006-04-11&atto.codiceRedazionale=006G0168&tipoDettaglio=multivigenza&qId=&tabID=0.5617783247471355&title=Atto%20multivigente&bloccoAggiornamentoBreadCrum b=true
What are the rules to be followed for the implementation of this tool?	Police, Carabinieri, Guardia di Finanza officers as well as officers belonging to the special structures of the Antimafia Investigative Direction (DIA- Direzione Investigativa Antimafia), Police and Carabinieri belonging to Antiterrorism department, Finance Police (Guardia di Finanza) competent to avoid financing of terrorism	Law of 16 March 2006, no. 146 (Article 9, sub 1, a and b) https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2006-04-11&atto.codiceRedazionale=006G0168&tipoDettaglio=multivigenza&qId=&tabID=0.5617783247471355&title=Atto%20multivigente&bloccoAggiornamentoBreadCrum b=true
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	1)The use of the tool is allowed by the top bodies of the law enforcement agency, or by its delegate in charge, at least, at the provincial level. In case of crimes related to immigration (Legislative Decree 286/1998) the authorisation to use the tool shall be in agreement with the Central Directorate of Immigration and Border Police. Before the use of the tool the competent Public Prosecutor shall be informed as well as during the use of the tool. 2) If, in order to find or arrest those who committed a crime police has to omit or delay their action, the competent Public Prosecutor shall be immediately informed. If the information was oral, a detailed report shall be sent to the Public Prosecutor within 48 hours. The Public Prosecutor leads the operation and informs the judicial competent authority of the place where the operation shall conclude or transit. The Public Prosecutor shall transmit relevant documents to the Chief Public Prosecutor at the Court of Appeal (Procuratore Generale della Corte d'Appello). In case of crimes related to mafia, the Anti-mafia Chief Prosecutor shall be informed.	Law of 16 March 2006, no. 146 (Article 9, sub 3, 4, 6, 7, 8) https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2006-04-11&atto.codiceRedazionale=006G0168&tipoDettaglio=multivigenza&qId=&tabID=0.5617783247471355&title=Atto%20multivigente&bloccoAggiornamentoBreadCrum b=true
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	1) The use of the tool is allowed by the top bodies of the law enforcement agency, or by its delegate in charge, at least, at the provincial level. In case of crimes related to immigration (Legislative Decree 286/1998) the authorisation to use the tool shall be in agreement with the Central Directorate of Immigration and Border Police. Before the use of the tool the competent Public Prosecutor shall be informed as well as during the use of the tool. 2) If, in order to find or arrest those who committed a crime police has to omit or delay their action, the competent Public Prosecutor shall be immediately informed. If the information was oral, a detailed report shall be sent to the Public Prosecutor within 48 hours. The Public Prosecutor leads the operation and informs the judicial competent authority of the place where the operation shall conclude or transit. The Public Prosecutor shall transmit relevant documents to the Chief Public Prosecutor at the Court of Appeal (Procuratore Generale della Corte d'Appello). In case of crimes related to mafia, the Anti-mafia Chief Prosecutor shall be informed	Law of 16 March 2006, no. 146 (Article 9, sub 3,4, 6, 7, 8) https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2006-04-11&atto.codiceRedazionale=006G0168&tipoDettaglio=multivigenza&qId=&tabID=0.5617783247471355&title=Atto%20multivigente&bloccoAggiornamentoBreadCrum b=true
What ongoing supervision is required for the use of this tool?	1) The use of the tool is allowed by the top bodies of the law enforcement agency, or by its delegate in charge, at least, at the provincial level. In case of crimes related to immigration (Legislative Decree 286/1998) the authorisation to use the tool shall be in agreement with the Central Directorate of Immigration and Border Police. Before the use of the tool the competent	

Relevant items	Provisions	Sources used
	Public Prosecutor shall be informed as well as during the use of the tool. 2) If, in order to find or arrest those who committed a crime police has to omit or delay their action, the competent Public Prosecutor shall be immediately informed. If the information was oral, a detailed report shall be sent to the Public Prosecutor within 48 hours. The Public Prosecutor leads the operation and informs the judicial competent authority of the place where the operation shall conclude or transit. The Public Prosecutor shall transmit relevant documents to the Chief Public Prosecutor at the Court of Appeal (Procuratore Generale della Corte d'Appello). In case of crimes related to mafia, the Anti-mafia Chief Prosecutor shall be informed	
Is there any national case law relating to the use of this tool in cross-border crime cases?	Supervision from Public Prosecutor and, If, in order to find or arrest those who committed a crime police has to omit or delay their action, Chief Public Prosecutor at the Court of Appeal and, if the crime is related to mafia, Anti-mafia Chief Prosecutor	Law of 16 March 2006, no. 146 (Article 9, sub 3, 4, 6, 7 and 8) https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2006-04-11&atto.codiceRedazionale=006G0168&tipoDettaglio=multivigenza&qId=&tabID=0.5617783247471355&title=Atto%20multivigente&bloccoAggiornamentoBreadcrumb=true
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	N/A	
Specific range of application of the tool	Article 203 Code of Criminal Procedure (C.p.p.)	https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.del.presidente.della.repubblica:1988-09-22;447
How is the tool defined?	no one	
For what types of crime can the tool be used?	the tool is defined as a mean of evidence	https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.del.presidente.della.repubblica:1988-09-22;447
Does national law allow this tool to be used in cross border cases?	cross crime areas	
What thresholds must be passed for the use of this tool?	cross border criminal investigations	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	LEAs	
What are the rules to be followed for the implementation of this tool?	Judicial Police, External Intelligence and Security Agency (AISE-Agenzia informazioni e sicurezza esterna), Internal Intelligence and Security Agency (AISI-Agenzia informazioni e sicurezza interna)	https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.del.presidente.della.repubblica:1988-09-22;447
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	no one- In the Italian legal system confidential information may only be used as a hint to start investigative enquiries (never as evidence); having said that, it is worth noting that the judge may not force the judicial police to reveal the names of informers, and if they are not examined as witnesses the information they provide may not be included in the case file or used.	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	the judge may not force the judicial police to reveal the names of informers in the interest of the informers	https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.del.presidente.della.repubblica:1988-09-22;447
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	

Source: Author's own elaboration

Latvia

Table 34 – Overview of national rules on investigative tools - Latvia

Relevant items	Provisions	Sources used
Controlled Delivery		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Procedure Law	https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law
How is the tool defined?	Controlled delivery is the movement of goods or other valuables (including substances, means of payment or other financial instruments) in the territory of Latvia or across the State borders and the control of persons associated with such movement the purpose of which is to prevent or detect criminal offences and to ascertain the persons committing such offences if information has been received or there are justified suspicions regarding the association of the goods or other valuables to be moved with criminal offences.	Operational activities Law Section 15 (1) Criminal Procedure Law. Link 1) https://vvc.gov.lv/index.php?route=product/category&path=60_109_111_112 and 2) https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjws9yA-JPvAhVB8xQKHQs8DCgQFjACegQIAxAD&url=http%3A%2F%2Fwww.vvc.gov.lv%2Fexport%2Fsites%2Fdefault%2Fdocs%2FLRTA%2FLikumi%2FInvestigatory_Operations.doc&usg=AOvVaw3kGXYVrYGzHtGdBfTvqMnf
For what types of crime can the tool be used?	illicit substances, means of payment or other financial instruments	Operational activities Law Section 15 (1) Criminal Procedure Law. Link 1) https://vvc.gov.lv/index.php?route=product/category&path=60_109_111_112 and 2) https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjws9yA-JPvAhVB8xQKHQs8DCgQFjACegQIAxAD&url=http%3A%2F%2Fwww.vvc.gov.lv%2Fexport%2Fsites%2Fdefault%2Fdocs%2FLRTA%2FLikumi%2FInvestigatory_Operations.doc&usg=AOvVaw3kGXYVrYGzHtGdBfTvqMnf
Does national law allow this tool to be used in cross border cases?	This tool is widely used within the borders and rarely used in cross-border cases which obliged Latvia to adhere to Schengen Convention laws	Operational activities Law Section 15 (1) Criminal Procedure Law. Link 1) https://vvc.gov.lv/index.php?route=product/category&path=60_109_111_112 and 2) https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjws9yA-JPvAhVB8xQKHQs8DCgQFjACegQIAxAD&url=http%3A%2F%2Fwww.vvc.gov.lv%2Fexport%2Fsites%2Fdefault%2Fdocs%2FLRTA%2FLikumi%2FInvestigatory_Operations.doc&usg=AOvVaw3kGXYVrYGzHtGdBfTvqMnf
What thresholds must be passed for the use of this tool?	If the body performing operational activities has at its disposal information with respect to specific persons (including where obtained as a result of an investigatory examination) and it provides a sufficient basis to suspect such persons of planning or committing a criminal offence or threatening interests of importance to the State, or such persons are being sought with respect to a criminal offence already committed, exercising of operational activities shall be initiated with respect to such persons.	Operational activities Law, Section 22 (1) Exercising of operational activities. Link 1) https://vvc.gov.lv/index.php?route=product/category&path=60_109_111_112 and 2) https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjws9yA-JPvAhVB8xQKHQs8DCgQFjACegQIAxAD&url=http%3A%2F%2Fwww.vvc.gov.lv%2Fexport%2Fsites%2Fdefault%2Fdocs%2FLRTA%2FLikumi%2FInvestigatory_Operations.doc&usg=AOvVaw3kGXYVrYGzHtGdBfTvqMnf
What types of stakeholder are involved in the implementation of this tool?	LEAs and Police Department	Operational activities Law Section 15 (1) 4, Criminal Procedure Law. Link 1) https://vvc.gov.lv/index.php?route=product/category&path=60_109_111_112 and 2) https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjws9yA-JPvAhVB8xQKHQs8DCgQFjACegQIAxAD&url=http%3A%2F%2Fwww.vvc.gov.lv%2Fexport%2Fsites%2Fdefault%2Fdocs%2FLRTA%2FLikumi%2FInvestigatory_Operations.doc&usg=AOvVaw3kGXYVrYGzHtGdBfTvqMnf
Which LEAs can use this tool?	The system of bodies performing operational activities consists of State security and defence institutions, institutions for maintaining public order, and other specially authorised State bodies which by law are granted the right to perform operational activities measures within the scope of their competence and whose specially authorised officials are entitled to carry out such activities in accordance with procedures laid down in this Law.	Operational activities Law Chapter 4 - Bodies Performing Operational Activities, their Rights, Obligations and Responsibilities, Section 25 (1). Link 1) https://vvc.gov.lv/index.php?route=product/category&path=60_109_111_112 and 2) https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjws9yA-JPvAhVB8xQKHQs8DCgQFjACegQIAxAD&url=http%3A%2F%2Fwww.vvc.gov.lv%2Fexport%2Fsites%2Fdefault%2Fdocs%2FLRTA%2FLikumi%2FInvestigatory_Operations.doc&usg=AOvVaw3kGXYVrYGzHtGdBfTvqMnf
What are the rules to be followed for the implementation of this tool?	1) Bodies performing operational activities shall perform only such investigatory activities laid down in this Law as are necessary to fulfil the tasks and attain the objectives laid down in law, and only within their competence as laid down in law. (2) The main directions of investigatory activities, their types, content, amount and intensity shall be determined by the head of the operational activities body, taking into account the investigatory and criminogenic situation and changes his or her sphere of activities, as well as	Operational activities Law, Chapter 4 - Competence of Bodies Performing Operational Activities and of their Officials, Section 26 (1), (2), (3) and (4). Link 1) https://vvc.gov.lv/index.php?route=product/category&path=60_109_111_112 and 2) https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjws9yA-JPvAhVB8xQKHQs8DCgQFjACegQIAxAD&url=http%3A%2F%2Fwww.vvc.gov.lv%2F

Relevant items	Provisions	Sources used
	the type and danger of the existing threat, in order to ensure the implementation of tasks laid down in law and the achievement of aims. (3) Officials of bodies performing operational activities are entitled to perform operational activities measures only to such extent as is prescribed in the laws regulating the rights and duties of officials of such bodies. (4) In the course of performing operational activities measures, officials of bodies performing operational activities are entitled to act overtly and covertly, to act directly (in person) and indirectly (with the assistance of other persons).	export%2Fsites%2Fdefault%2Fdocs%2FLRTA%2FLikumi%2FInvestigatory_Operations.doc&usg=AOvVaw3kGXYVrYGzHtGdBfTvqMnf
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	YES. (1) Operational activities shall be organised and performed on a lawful basis, observing overall human rights, and in co-operation with and relying on the assistance of the general public. 2) Operational activities measures, and the manner, scope and intensity of the conducting thereof, shall be commensurate to the form and danger level of the threat. Investigatory tasks shall be conducted so as to interfere as little as possible in the sphere of human rights.	Section 4 (1) and (3). Principles of Operational activities of Operational activities Law. Link 1) https://vvc.gov.lv/index.php?route=product/category&path=60_109_111_112 and 2) https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjws9yA-JPvAhVB8xQKHQs8DCgQFjACegQIAxAD&url=http%3A%2F%2Fwww.vvc.gov.lv%2Fexport%2Fsites%2Fdefault%2Fdocs%2FLRTA%2FLikumi%2FInvestigatory_Operations.doc&usg=AOvVaw3kGXYVrYGzHtGdBfTvqMnf
What authorisation is needed for the use of this tool?	Controlled delivery shall be performed on the basis of a decision of an official of an investigatory operations body, which has been approved by a prosecutor.	section 15-1 (4) of Operational Activities law
What ongoing supervision is required for the use of this tool?	(1) Monitoring regarding the conformity to law of operational activities shall be performed by the Prosecutor General and by prosecutors specially authorised by the Prosecutor General. In performing monitoring they are entitled to acquaint themselves with documents, materials and information at any stage of operational activities as is available to the operational activities institution. Covert information and its sources shall be revealed only to the Prosecutor General, but to the prosecutors specially authorised by the Prosecutor General – only with the permission of the head of the operational activities institution. (2) In order to take a decision with respect to operational activities measures mentioned in this Law the performance of which requires approval by a judge, the judge is entitled to acquaint himself or herself with those documents, materials and information available to the operational activities institution, upon which the necessity for the specific operational activities measures is based. The covert information and the sources of such shall be revealed to the judge only with the permission of the head of the operational activities institution.	Operational activities Law, Chapter 4, Section 35 (1) and (2) Monitoring of Operational Activities. Link 1) https://vvc.gov.lv/index.php?route=product/category&path=60_109_111_112 and 2) https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjws9yA-JPvAhVB8xQKHQs8DCgQFjACegQIAxAD&url=http%3A%2F%2Fwww.vvc.gov.lv%2Fexport%2Fsites%2Fdefault%2Fdocs%2FLRTA%2FLikumi%2FInvestigatory_Operations.doc&usg=AOvVaw3kGXYVrYGzHtGdBfTvqMnf
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Data available on the number of times this tool has been used for SOC cases	N/A	
Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	The national law does not include the hot pursuit as investigation tool because it is used rarely. But Latvia being a member of Schengen Convention which is binding for all member states. The Convention has the specific set of laws to carry out these tool.	The previous study confirms this findings. To quote from the previous study "Cross-border hot pursuit is not a measure of planned nature. Is can be concluded from the wording of Schengen convention, chapter III "Police and security". It cannot be estimated whether such situations are frequent or rare as they are unexpected and require immediate reaction. The necessary authorisation is included in the guidelines of Schengen convention as explanations of the member states and they are of binding nature."
How is the tool defined?	N/A	
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	

Relevant items	Provisions	Sources used
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Procedure Law, Operation Activities law	https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law
How is the tool defined?	A witness is a person who has been invited, in accordance with the procedures laid down in law, to provide information (testify) regarding the circumstances to be proven in criminal proceedings and the facts and auxiliary facts related to such circumstances.	Chapter 7, section 109 (1) of criminal procedure law. https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross border cases?	NO. Witnessing has to be within national jurisdictions hence cannot applicable cross-border cases	Section 1 of operational activities law
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	LEAs and Police Department	Section 8 (1,2,3,4) of criminal procedure law
Which LEAs can use this tool?	LEAs and Police Department	- Section 8 (1,2,3,4) of criminal procedure law - Section 8 (1,2,3,4) of criminal procedure law
What are the rules to be followed for the implementation of this tool?	(1) The Prosecutor General or a court shall take a decision regarding special protection of a person testifying in criminal proceedings after becoming acquainted with a submission of the person, a proposal of the performer of procedures and the materials of the criminal matter, as well as, if necessary, shall hear the threatened person, his or her representative or counsel. (2) A court may also take a decision regarding special protection of a person testifying in criminal proceedings on its own initiative if the necessity to prescribe special protection of the person has arisen during the adjudication procedure and the consent of such person or his or her legal representative has been received. (3) Prior to the taking of a decision, the Prosecutor General or a court may assign a special protection institution to perform an inspection and provide an opinion regarding the feasibility of a threat and protection measures within a time period of no longer than five days. (4) Upon the examination of a submission of another person to be protected, the head of a special protection institution shall take a decision regarding the prescription of special protection for the person. If necessary, the head of the special protection institution shall organise an assessment of the indicated conditions, threat and potential persons who make threats and hear the threatened person or his or her legal representative.	Section 8 (1,2,3,4) of criminal procedure law
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	all the rights i.e. to have court, to opt out as witness etc. is given in the section 110	Section 110 - 1 to 5 - Rights of a Witness of criminal procedure law
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	pls refer to D40	
What ongoing supervision is required for the use of this tool?	there is no need for ongoing supervision. Unless in emergency cases, In such case, a performer of procedures shall immediately, but not later than within a time period of 10 days, send a proposal to the Prosecutor General	Section 9 (2) of criminal procedure law
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	

Relevant items	Provisions	Sources used
Surveillance		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Procedure Law	https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law
Specific range of application of the tool	N/A	
How is the tool defined?	Surveillance and tracking of a person without the information thereof shall be performed, on the basis of a decision of an investigating judge, if there are grounds to believe that the behaviour of the person, or his or her contact with other persons, may contain information regarding facts included in circumstances to be proven, for a term up to 30 days which an investigating judge may extend, if necessary.	Criminal Procedure Law, Chapter 11, Section 223 (1). https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law
For what types of crime can the tool be used?	The investigative tools are never used separately. It depends upon what kind of offence is being investigated.	Section 215 of Criminal Procedure Law
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	(1) If a body performing operational activities has available well-founded information regarding a criminal offence in preparation or having been committed by persons, or regarding other unlawful acts, or a threat to interests of importance to the State, the surveillance (tracing) of such persons and persons associated with them is permitted. (2) In order to obtain or verify information regarding unlawful acts or a threat to interests of importance to the State, the surveillance of various stationary and mobile facilities and surveillance (tracing) of persons associated with such is permitted. (3) In order to uncover and avert possible threats to facilities of importance to the State, preventive investigatory surveillance of such facilities is permitted.	Investigatory Surveillance (Tracing). Operational activities Law, Chapter 2, Section 10 (1), (2), (3) and (4). Link 1) https://vvc.gov.lv/index.php?route=product/category&path=60_109_111_112 and 2) https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjws9yA-JPvAhVB8xQKHQs8DCgQFjACegQIAxAD&url=http%3A%2F%2Fwww.vvc.gov.lv%2Fexport%2Fsites%2Fdefault%2Fdocs%2FLRTA%2FLikumi%2FInvestigatory_Operations.doc&usg=AOvVaw3kGXYVrYGzHtGdBfTvqMnf
What types of stakeholder are involved in the implementation of this tool?	LEAs and Police Department	Section 8 (1,2,3,4) of criminal procedure law
Which LEAs can use this tool?	Surveillance of an object or a site shall be performed, on the basis of a decision of an investigating judge along with police department.	Criminal Procedure Law, Chapter 11, Section 224. https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law
What are the rules to be followed for the implementation of this tool?	In case of audio-video surveillance - 1) a judge of the Supreme Court specially authorised by the Chairperson of the Supreme Court - for the control of correspondence, control of means of communication, audio control of a site or a person, video control of a site, control of data in an electronic information system, and control of the content of broadcast data; 2) prosecutors specially authorised by the Prosecutor General - for the surveillance and tracing of a person, surveillance of an object, for a special investigative experiment, for the obtaining in a special manner of samples necessary for a comparative study, and for the control of criminal activity.	Chapter 86, Transitional Provisions 13 (1,2). https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	1) Bodies performing operational activities shall perform only such investigatory activities laid down in this Law as are necessary to fulfil the tasks and attain the objectives laid down in law, and only within their competence as laid down in law. (2) The main directions of investigatory activities, their types, content, amount and intensity shall be determined by the head of the operational activities body, taking into account the investigatory and criminogenic situation and changes his or her sphere of activities, as well as the type and danger of the existing threat, in order to ensure the implementation of tasks laid down in law and the achievement of aims. (3) Officials of bodies performing operational activities are entitled to perform operational activities measures only to such extent as is prescribed in the laws regulating the rights and duties of officials of such bodies. (4) In the course of performing operational activities measures, officials of bodies performing operational activities are entitled to act overtly and covertly, to act directly (in person) and indirectly (with the assistance of other persons).	Operational activities Law, Chapter 4 - Competence of Bodies Performing Operational Activities and of their Officials, Section 26 (1), (2), (3) and (4). Link 1) https://vvc.gov.lv/index.php?route=product/category&path=60_109_111_112 and 2) https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjws9yA-JPvAhVB8xQKHQs8DCgQFjACegQIAxAD&url=http%3A%2F%2Fwww.vvc.gov.lv%2Fexport%2Fsites%2Fdefault%2Fdocs%2FLRTA%2FLikumi%2FInvestigatory_Operations.doc&usg=AOvVaw3kGXYVrYGzHtGdBfTvqMnf
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	YES. (1) Operational activities shall be organised and performed on a lawful basis, observing overall human rights, and in co-operation with and relying on the assistance of the general public. 2) Operational activities measures, and the manner, scope and intensity of the conducting thereof, shall be commensurate to the form and danger level of the threat. Investigatory tasks shall be conducted so as to interfere as little as possible in the sphere of human rights.	Section 4 (1) and (3). Principles of Operational activities of Operational activities Law. Link 1) https://vvc.gov.lv/index.php?route=product/category&path=60_109_111_112 and 2) https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjws9yA-JPvAhVB8xQKHQs8DCgQFjACegQIAxAD&url=http%3A%2F%2Fwww.vvc.gov.lv%2Fexport%2Fsites%2Fdefault%2Fdocs%2FLRTA%2FLikumi%2FInvestigatory_Operations.doc&usg=AOvVaw3kGXYVrYGzHtGdBfTvqMnf
What ongoing supervision is required for the use of this tool?	Surveillance shall be performed on the basis of a decision of an official of an investigatory operations body, which has been approved by a prosecutor.	section 15-1 (4) of Operational Activities law
Is there any national case law relating to the use of this tool in cross-border crime cases?	(1) Monitoring regarding the conformity to law of operational activities shall be performed by the Prosecutor General and by prosecutors specially authorised by the Prosecutor General. In performing monitoring they are entitled to acquaint themselves with documents, materials and	Operational activities Law, Chapter 4, Section 35 (1) and (2) Monitoring of Operational Activities. Link 1) https://vvc.gov.lv/index.php?route=product/category&path=60_109_111_112 and

Relevant items	Provisions	Sources used
	information at any stage of operational activities as is available to the operational activities institution. Covert information and its sources shall be revealed only to the Prosecutor General, but to the prosecutors specially authorised by the Prosecutor General – only with the permission of the head of the operational activities institution. (2) In order to take a decision with respect to operational activities measures mentioned in this Law the performance of which requires approval by a judge, the judge is entitled to acquaint himself or herself with those documents, materials and information available to the operational activities institution, upon which the necessity for the specific operational activities measures is based. The covert information and the sources of such shall be revealed to the judge only with the permission of the head of the operational activities institution.	2) https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjws9yA-JPvAhVB8xQKHQs8DCgQFjACegQIAxAD&url=http%3A%2F%2Fwww.vvc.gov.lv%2Fexport%2Fsites%2Fdefault%2Fdocs%2FLRTA%2FLikumi%2FInvestigatory_Operations.doc&usg=AOvVaw3kGXYVrYGzHtGdBfTvqMnf
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Undercover / covert operations		
Relevant documents (legal and non-legal) that define the functioning of the tool	Operational Guidelines Act	https://vvc.gov.lv/index.php?route=product/category&path=60_109_111_112 and 2) https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjws9yA-JPvAhVB8xQKHQs8DCgQFjACegQIAxAD&url=http%3A%2F%2Fwww.vvc.gov.lv%2Fexport%2Fsites%2Fdefault%2Fdocs%2FLRTA%2FLikumi%2FInvestigatory_Operations.doc&usg=AOvVaw3kGXYVrYGzHtGdBfTvqMnf
How is the tool defined?	Investigatory detective work is investigatory measures that are performed in public places directly (in person) by an official of the body performing operational activities in order to determine, by surveillance and tracing, facts, things and persons related to criminal activity, to prevent or uncover criminal offences, threats to interests of importance to the State, State security and defence and to search for suspects, accused persons, convicted persons and missing persons	Operational activities Law, Chapter 2, Section 16 (1) Link 1) https://vvc.gov.lv/index.php?route=product/category&path=60_109_111_112 and 2) https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjws9yA-JPvAhVB8xQKHQs8DCgQFjACegQIAxAD&url=http%3A%2F%2Fwww.vvc.gov.lv%2Fexport%2Fsites%2Fdefault%2Fdocs%2FLRTA%2FLikumi%2FInvestigatory_Operations.doc&usg=AOvVaw3kGXYVrYGzHtGdBfTvqMnf
For what types of crime can the tool be used?	The investigative tools are never used separately. It depends upon what kind of offence is being investigated.	Section 215 of Criminal Procedure Law
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	Investigatory detective work may be performed either overtly or concealing affiliation with the body performing investigatory operations; in the course of such, with the permission of the head or deputy head of the institution performing the investigatory operations, contact may be established with persons eliciting the investigatory interest.	Operational activities Law, Chapter 2, Section 16 (2) Link 1) https://vvc.gov.lv/index.php?route=product/category&path=60_109_111_112 and 2) https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjws9yA-JPvAhVB8xQKHQs8DCgQFjACegQIAxAD&url=http%3A%2F%2Fwww.vvc.gov.lv%2Fexport%2Fsites%2Fdefault%2Fdocs%2FLRTA%2FLikumi%2FInvestigatory_Operations.doc&usg=AOvVaw3kGXYVrYGzHtGdBfTvqMnf
What types of stakeholder are involved in the implementation of this tool?	LEAs and Police Department	Section 8 (1,2,3,4) of criminal procedure law
Which LEAs can use this tool?	permission of the head or deputy head of the institution performing the investigatory operations with police department	Operational activities Law, Chapter 2, Section 16 (3) Link 1) https://vvc.gov.lv/index.php?route=product/category&path=60_109_111_112 and 2) https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjws9yA-JPvAhVB8xQKHQs8DCgQFjACegQIAxAD&url=http%3A%2F%2Fwww.vvc.gov.lv%2Fexport%2Fsites%2Fdefault%2Fdocs%2FLRTA%2FLikumi%2FInvestigatory_Operations.doc&usg=AOvVaw3kGXYVrYGzHtGdBfTvqMnf
What are the rules to be followed for the implementation of this tool?	In carrying out the tasks of the investigatory process, officials of the body performing investigatory operations are entitled with the approval of the prosecutor to perform investigatory detective work by becoming involved in a criminal environment (directly or under false identity), establishing contacts with persons set out in the investigative record and persons associated with them. Such activity and the identity of the officials is an official secret.	Operational activities Law, Chapter 2, Section 16 (3) Link 1) https://vvc.gov.lv/index.php?route=product/category&path=60_109_111_112 and 2) https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjws9yA-JPvAhVB8xQKHQs8DCgQFjACegQIAxAD&url=http%3A%2F%2Fwww.vvc.gov.lv%2Fexport%2Fsites%2Fdefault%2Fdocs%2FLRTA%2FLikumi%2FInvestigatory_Operations.doc&usg=AOvVaw3kGXYVrYGzHtGdBfTvqMnf
Safeguards provided by national criminal laws to protect the rights of the	YES. (1) Operational activities shall be organised and performed on a lawful basis, observing overall human rights, and in co-operation with and relying on the assistance of the general public. 2) Operational activities measures, and the manner, scope and intensity of the conducting	Section 4 (1) and (3). Principles of Operational activities of Operational activities Law. Link 1) https://vvc.gov.lv/index.php?route=product/category&path=60_109_111_112 and

Relevant items	Provisions	Sources used
individuals, ensure proportionality, and protect rule of law (if any)	thereof, shall be commensurate to the form and danger level of the threat. Investigatory tasks shall be conducted so as to interfere as little as possible in the sphere of human rights.	2) https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjws9yA-JPvAhVB8xQKHQs8DCgQFjACegQIAxAD&url=http%3A%2F%2Fwww.vvc.gov.lv%2Fexport%2Fsites%2Fdefault%2Fdocs%2FLRTA%2FLikumi%2FInvestigatory_Operations.doc&usg=AOvVaw3kGXYVrYGzHtGdBfTvqMnf
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	With the permission of the head or deputy head of the institution performing the investigatory operations, this tool can be used.	Section 16 (2) of criminal procedure law
What ongoing supervision is required for the use of this tool?	(1) Monitoring regarding the conformity to law of operational activities shall be performed by the Prosecutor General and by prosecutors specially authorised by the Prosecutor General. In performing monitoring they are entitled to acquaint themselves with documents, materials and information at any stage of operational activities as is available to the operational activities institution. Covert information and its sources shall be revealed only to the Prosecutor General, but to the prosecutors specially authorised by the Prosecutor General – only with the permission of the head of the operational activities institution. (2) In order to take a decision with respect to operational activities measures mentioned in this Law the performance of which requires approval by a judge, the judge is entitled to acquaint himself or herself with those documents, materials and information available to the operational activities institution, upon which the necessity for the specific operational activities measures is based. The covert information and the sources of such shall be revealed to the judge only with the permission of the head of the operational activities institution.	Operational activities Law, Chapter 4, Section 35 (1) and (2) Monitoring of Operational Activities. Link 1) https://vvc.gov.lv/index.php?route=product/category&path=60_109_111_112 and 2) https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjws9yA-JPvAhVB8xQKHQs8DCgQFjACegQIAxAD&url=http%3A%2F%2Fwww.vvc.gov.lv%2Fexport%2Fsites%2Fdefault%2Fdocs%2FLRTA%2FLikumi%2FInvestigatory_Operations.doc&usg=AOvVaw3kGXYVrYGzHtGdBfTvqMnf
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	Operational Activity Laws	https://vvc.gov.lv/index.php?route=product/category&path=60_109_111_112 and 2) https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjws9yA-JPvAhVB8xQKHQs8DCgQFjACegQIAxAD&url=http%3A%2F%2Fwww.vvc.gov.lv%2Fexport%2Fsites%2Fdefault%2Fdocs%2FLRTA%2FLikumi%2FInvestigatory_Operations.doc&usg=AOvVaw3kGXYVrYGzHtGdBfTvqMnf
Specific range of application of the tool	normal person appointed by police which was or will be trained in special skills	Operational activities Law, Chapter 5, Section 30 (1) and (2).
How is the tool defined?	Authorised officials of bodies performing operational activities have the right, on a voluntary and mutual trust basis, to recruit persons, who have legal capacity, as covert helpers in operational activities.	Operational activities Law, Chapter 5, Section 30 (1). Link 1) https://vvc.gov.lv/index.php?route=product/category&path=60_109_111_112 and 2) https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjws9yA-JPvAhVB8xQKHQs8DCgQFjACegQIAxAD&url=http%3A%2F%2Fwww.vvc.gov.lv%2Fexport%2Fsites%2Fdefault%2Fdocs%2FLRTA%2FLikumi%2FInvestigatory_Operations.doc&usg=AOvVaw3kGXYVrYGzHtGdBfTvqMnf
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	If the body performing operational activities has at its disposal information with respect to specific persons (including where obtained as a result of an investigatory examination) and it provides a sufficient basis to suspect such persons of planning or	Investigatory Surveillance (Tracing). Operational activities Law, Chapter 2, Section 10 (1), (2), (3) and (4). Link 1) https://vvc.gov.lv/index.php?route=product/category&path=60_109_111_112 and 2) https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjws9yA-JPvAhVB8xQKHQs8DCgQFjACegQIAxAD&url=http%3A%2F%2Fwww.vvc.gov.lv%2Fexport%2Fsites%2Fdefault%2Fdocs%2FLRTA%2FLikumi%2FInvestigatory_Operations.doc&usg=AOvVaw3kGXYVrYGzHtGdBfTvqMnf
What types of stakeholder are involved in the implementation of this tool?	The National Security Committee of the <i>Saeima</i> is entitled to hear the reports and accounts of the heads of institutions performing operational activities, examine the results of inspections of such institutions,	Section 34 (2) of operational activities act

Relevant items	Provisions	Sources used
Which LEAs can use this tool?	State Police department, Judge can give order to investigate, Financial Investigative Unit can give the order	Investigatory Surveillance (Tracing). Operational activities Law, Chapter 2, Section 09 (1), (2), (3) and (4). Link 1) https://vvc.gov.lv/index.php?route=product/category&path=60_109_111_112 and 2) https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjws9yA-JPvAhVB8xQKHQs8DCgQFjACegQIAxAD&url=http%3A%2F%2Fwww.vvc.gov.lv%2Fexport%2Fsites%2Fdefault%2Fdocs%2FLRTA%2FLikumi%2FInvestigatory_Operations.doc&usg=AOvVaw3kGXYVrYGzHtGdBfTvqMnf
What are the rules to be followed for the implementation of this tool?	1) Bodies performing operational activities shall perform only such investigatory activities laid down in this Law as are necessary to fulfil the tasks and attain the objectives laid down in law, and only within their competence as laid down in law. (2) The main directions of investigatory activities, their types, content, amount and intensity shall be determined by the head of the operational activities body, taking into account the investigatory and criminogenic situation and changes his or her sphere of activities, as well as the type and danger of the existing threat, in order to ensure the implementation of tasks laid down in law and the achievement of aims. (3) Officials of bodies performing operational activities are entitled to perform operational activities measures only to such extent as is prescribed in the laws regulating the rights and duties of officials of such bodies. (4) In the course of performing operational activities measures, officials of bodies performing operational activities are entitled to act overtly and covertly, to act directly (in person) and indirectly (with the assistance of other persons).	Operational activities Law, Chapter 4 - Competence of Bodies Performing Operational Activities and of their Officials, Section 26 (1), (2), (3) and (4). Link 1) https://vvc.gov.lv/index.php?route=product/category&path=60_109_111_112 and 2) https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjws9yA-JPvAhVB8xQKHQs8DCgQFjACegQIAxAD&url=http%3A%2F%2Fwww.vvc.gov.lv%2Fexport%2Fsites%2Fdefault%2Fdocs%2FLRTA%2FLikumi%2FInvestigatory_Operations.doc&usg=AOvVaw3kGXYVrYGzHtGdBfTvqMnf
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	If as a result of covert co-operation the life, health, or financial and other lawful interests of the covert helper or his or her family members are endangered, security measures necessary to avert such danger, including change of domicile and personal identification documents, shall be undertaken in good time.	Section 31 (4) of operational activities law
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	The prosecution has the overall authority to authorise use of tool. Department head of state, national police etc. can also start using tool.	Section 31 (4) of operational activities law
What ongoing supervision is required for the use of this tool?	(1) Monitoring regarding the conformity to law of operational activities shall be performed by the Prosecutor General and by prosecutors specially authorised by the Prosecutor General. In performing monitoring they are entitled to acquaint themselves with documents, materials and information at any stage of operational activities as is available to the operational activities institution. Covert information and its sources shall be revealed only to the Prosecutor General, but to the prosecutors specially authorised by the Prosecutor General – only with the permission of the head of the operational activities institution. (2) In order to take a decision with respect to operational activities measures mentioned in this Law the performance of which requires approval by a judge, the judge is entitled to acquaint himself or herself with those documents, materials and information available to the operational activities institution, upon which the necessity for the specific operational activities measures is based. The covert information and the sources of such shall be revealed to the judge only with the permission of the head of the operational activities institution.	Operational activities Law, Chapter 4, Section 35 (1) and (2) Monitoring of Operational Activities. Link 1) https://vvc.gov.lv/index.php?route=product/category&path=60_109_111_112 and 2) https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjws9yA-JPvAhVB8xQKHQs8DCgQFjACegQIAxAD&url=http%3A%2F%2Fwww.vvc.gov.lv%2Fexport%2Fsites%2Fdefault%2Fdocs%2FLRTA%2FLikumi%2FInvestigatory_Operations.doc&usg=AOvVaw3kGXYVrYGzHtGdBfTvqMnf
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	

Source: Author's own elaboration

Liechtenstein

Table 35 – Overview of national rules on investigative tools - Liechtenstein

Relevant items	Provisions	Sources used
Controlled Delivery		
Relevant documents (legal and non-legal) that define the functioning of the tool	Liechtensteinisches Landesgesetzblatt über die internationale Rechtshilfe in Strafsachen (Rechtshilfegesetz, RHG) European Convention on Extradition (Europäisches Auslieferungsübereinkommen)	- Liechtensteinisches Landesgesetzblatt über die internationale Rechtshilfe in Strafsachen (Rechtshilfegesetz, RHG) https://www.gesetze.li/konso/2000215000 - Europäisches Auslieferungsabkommen

Relevant items	Provisions	Sources used
		https://www.gesetze.li/konso/pdf/1970029000?version=1
How is the tool defined?		
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Data available on the number of times this tool has been used for SOC cases	Liechtensteinisches Landesgesetzblatt über die internationale Rechtshilfe in Strafsachen (Rechtshilfegesetz, RHG) European Convention on Extradition (Europäisches Auslieferungsübereinkommen)	- Liechtensteinisches Landesgesetzblatt über die internationale Rechtshilfe in Strafsachen (Rechtshilfegesetz, RHG) https://www.gesetze.li/konso/2000215000 - Europäisches Auslieferungsabkommen https://www.gesetze.li/konso/pdf/1970029000?version=1
Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	Liechtenstein is part of the Schengen Convention as agreed in the Schengen Association Agreement and will therefore apply the relevant provisions of these instruments. Multilateral agreement exists for interstate police cooperation with the bordering countries Switzerland and Austria.	- Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22011A0618(01)&from=EN - Agreement with the European Police Office (Europol) https://www.gesetze.li/konso/2013405000?search_text=schengen&search_loc=text&lrmr=&lgblid_von=&observe_date=16.03.2021 - Agreement with Switzerland and Austria https://www.gesetze.li/konso/2017186000?search_text=grenz%C3%BCberschreitende%20polizeiliche%20Zusammenarbeit&search_loc=text&lrmr=&lgblid_von=&observe_date=12.03.2021
How is the tool defined?	N/A	
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	

Relevant items	Provisions	Sources used
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Date: 7 March 2014 Summary: On the basis of an arrest warrant issued by the Sofia City Court Prosecutor's Office on July 20, 2007, the complainant was issued a European Arrest Warrant for his arrest. On the occasion of a border control at the customs office in Schaanwald, the complainant was taken into custody upon entering Liechtenstein from Austria. On the basis of a request for legal assistance from the Prosecutor General's Office of the Republic of Bulgaria, the extradition of the complainant in the preliminary proceedings conducted by the Sofia Public Prosecutor's Office for a criminal offense under Bulgarian criminal procedure law was declared admissible by decision of the Supreme Court. The complainant was extradited to Bulgaria, whereupon the complainant objected to the proceedings. The individual complaint is not upheld. The complainant's constitutional rights and rights guaranteed by the ECHR are not violated by the contested decision of the Princely Supreme Court.	- The published judgments and decisions of the State Court of Liechtenstein - StGH 2014/37 https://www.gerichtsentscheidungen.li/default.aspx?z=4Uv7hYKsjbzE6dJ4-cAAKzefXKLIByb38wkwDpYac8A4VPQ-6QCRPIF6d51qX-cXk2vRUuucIVvHgFdjpaytOaObYTFBbVk93OO_YF0KBI81
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	Liechtenstein is part of the Schengen Convention as agreed in the Schengen Association Agreement and will therefore apply the relevant provisions of these instruments. Multilateral agreement exists for interstate police cooperation with the bordering countries Switzerland and Austria.	- Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22011A0618(01)&from=EN - Agreement with the European Police Office (Europol) https://www.gesetze.li/konso/2013405000?search_text=schengen&search_loc=txt&lrmr=&lglid_von=&observe_date=16.03.2021 - Agreement with Switzerland and Austria https://www.gesetze.li/konso/2017186000?search_text=grenz%C3%BCberschreitende%20polizeiliche%20Zusammenarbeit&search_loc=text&lrmr=&lglid_von=&observe_date=12.03.2021
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	Witness Protection is part of the Law on the National Police (Police Act; PolG)	https://www.gesetze.li/konso/pdf/1989.048
How is the tool defined?	This law regulates the tasks, organisation, rights and duties of the state police. According to Art. 2 letter p) of PolG, the provincial police shall protect persons who assist in criminal proceedings in the investigation of a serious criminal offence and are therefore particularly endangered, as well as any endangered relatives (section 72 of the Criminal Code) of such persons (witness protection).	Art. 2 letter p) PolG
For what types of crime can the tool be used?	cross crime areas	PolG
Does national law allow this tool to be used in cross border cases?	The Government may decide to hand over a person referred to in Article 2(1)(p) to a foreign country within the framework of witness protection or to take over such a person from a foreign country if it is indispensable to safeguard substantial security interests of that person.	Art. 35a para. 5 PolG
What thresholds must be passed for the use of this tool?	There is no maximum term of imprisonment defined in this law.	
What types of stakeholder are involved in the implementation of this tool?	LEAs	PolG
Which LEAs can use this tool?	State Police	Art. 30d PolG
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	

Relevant items	Provisions	Sources used
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Surveillance		
Relevant documents (legal and non-legal) that define the functioning of the tool	Code of Criminal Procedure of 18 October 1987 (StPO) (Strafprozessordnung vom 18. Oktober 1988 (StPO))	- Code of Criminal Procedure in the Official Language (German) https://www.gesetze.li/konso/1988.62 - Unofficial English Translation https://www.legislationline.org/download/id/8270/file/Liechtenstein_Criminal_Procedure_Code_1987_am2017_en.pdf
Specific range of application of the tool	Surveillance of electronic communication	
How is the tool defined?	Surveillance of electronic communication	- LGBI CCP § 103 § 103
For what types of crime can the tool be used?	Cross crime areas	
Does national law allow this tool to be used in cross border cases?	Ordering the surveillance of electronic communication including the recording of its content shall be admissible only where it is to be expected that this will further the investigation of a punishable act committed with intent and subject to a penalty of more than one year of imprisonment	§ 103
What thresholds must be passed for the use of this tool?	LEA	§ 103
What types of stakeholder are involved in the implementation of this tool?	The National Police shall be asked to implement the surveillance of electronic communication in cooperation with the providers in terms of the Communication Act (§ 10). There shall be no notification of parties or other participants of the proceedings for the time being.	§ 103
Which LEAs can use this tool?	Ordering the surveillance of electronic communication shall be admissible only if the holder of the communication equipment is himself strongly suspect of having committed the offence, or there are reasons to assume that a person strongly suspect of the offence is staying with the holder of the equipment or is going to contact him using the equipment, unless the holder is one of the persons listed in § 107(1)(2), or the holder of the equipment expressly agrees to surveillance.	§ 103
What are the rules to be followed for the implementation of this tool?	The surveillance of electronic communication may be ordered by the investigating judge, but he shall immediately obtain the approval of the President of the Court of Appeal. If such consent is denied, the investigating judge shall immediately cancel the order and have the recordings destroyed. The ordered surveillance shall be limited to three months. If the requirement of surveillance continues to exist after that period has expired, the authorisation procedure shall be repeated.	§ 103
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Date: 18 January 2011 Summary: The Liechtenstein regional court submitted a request for mutual legal assistance to the Swiss federal criminal police "to carry out surveillance of electronic communications measures ordered on Swiss territory or to forward this request for mutual legal assistance to the competent Swiss law enforcement authority." The request for legal assistance of 13 October 2008 was ultimately approved by the competent Swiss legal assistance authorities in the canton of Schwyz, the public prosecutor's office of the canton of Schwyz, only insofar as "marginal data collection" (location survey and subscriber identification) had been requested, but not insofar as the recording of conversations (real-time monitoring) had also been requested. As a result of a merely provisional order and implementation, data were already transmitted to the Liechtenstein National Police or the Regional Court before definitive approval was granted by the Swiss authorities. However, the legal assistance was subsequently not approved with regard to the recording of call content - in contrast to the recording of call data and location determination. The Swiss authorities came to the conclusion (cf. ON 141 AS 749 f.) that domestic formal requirements were not met with regard to the recording of the conversations, which is why mutual assistance was refused in this regard and the destruction of the data already transmitted to the Liechtenstein prosecution authorities was requested.	- The published judgments and decisions of the State Court of Liechtenstein - StGH 2011/027 https://www.gerichtsentscheidungen.li/default.aspx?z=xnieyBhDZL4iTSTMd4EvEOggci3IswpFqF1CdSS8yN7weIBL8G_tzVYVzf3Q_KT9VkaLlerErMY-oy7MPjas6bIZUwKeAOW7CQyaUu-i2uiejMIGJuJEayqAx5pXMiJxqs50

Relevant items	Provisions	Sources used
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	Code of Criminal Procedure of 18 October 1987 (StPO) (Strafprozessordnung vom 18. Oktober 1988 (StPO))	- Code of Criminal Procedure in the Official Language (German) https://www.gesetze.li/konso/1988.62 - Unofficial English Translation https://www.legislationline.org/download/id/8270/file/Liechtenstein_Criminal_Procedure_Code_1987_am2017_en.pdf
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	- Surveillance of electronic communication	LGBI CCP § 103
Undercover / covert operations		
Relevant documents (legal and non-legal) that define the functioning of the tool	Code of Criminal Procedure of 18 October 1987 (StPO) (Strafprozessordnung vom 18. Oktober 1988 (StPO))	Official Language (German) 1988062000 (gesetze.li) Unofficial English Translation https://www.legislationline.org/download/id/8270/file/Liechtenstein_Criminal_Procedure_Code_1987_am2017_en.pdf
How is the tool defined?	Observation (Surveillance) Undercover investigation Secretly monitoring the behaviour of a person Fictitious transactions An undercover transaction in terms of this Act shall be the attempted or apparent commission of offences as far as these consist in the acquisition, obtainment, holding, import, export, or transit of items or assets that have been stolen, originate from a crime or are dedicated to committing a crime, or whose possession is absolutely prohibited.	§ 104a § 104b § 104c
For what types of crime can the tool be used?	Cross crime areas.	
Does national law allow this tool to be used in cross border cases?	Surveillance: As far as surveillance is to be carried out over a period of more than 48 hours, it shall be admissible only if there is the suspicion of an offence which has been committed with intent and which is subject to a penalty of more than one year of imprisonment Undercover Investigation: A systematic long-term undercover investigation shall be admissible only where the investigation of an offence which was committed with intent and which is subject to a penalty of more than one year or the prevention of an offence planned in the framework of a criminal or terrorist organisation (§§ 278 to 278b StGB) would otherwise be rendered substantially more difficult.	§ 104a § 104b
What thresholds must be passed for the use of this tool?	Investigating judge, National Police	§ 104a, § 104b, § 104c
What types of stakeholder are involved in the implementation of this tool?	Surveillance The National Police shall have the right to secretly monitor the behaviour of a person (surveillance) if this may further the investigation of an offence or the ascertainment of an accused's whereabouts. Undercover Investigation: The National Police may on their own initiative employ their officers or other persons - who will neither disclose their official capacity or their mission nor let it be known (undercover investigation) - on their behalf if this may further the investigation of an offence. Fictitious Transactions: On application of the Prosecution Service and after a ruling to such effect has been issued by the Court of Justice, the National Police shall have the right to conduct an undercover transaction (Para. 2) if otherwise the investigation of a crime (§ 17(1) StGB) or the securing of items or assets originating from a crime or threatened by confiscation (§ 19a StGB), forfeiture (§ 20 StGB), extended forfeiture (§ 20b StGB), or seizure (§ 26 StGB) would be made substantially more difficult. Under these requirements, it shall also be admissible to contribute to the carrying out of an undercover transaction by third parties (§ 12 third case StGB)	§ 104a § 104b § 104c
Which LEAs can use this tool?	Surveillance pursuant to Para. (3) shall be ordered by the investigating judge on application of the Prosecution Service for such time as is probably required to achieve its purpose, but for no longer than three months. The National Police shall be asked to carry out the surveillance (§ 10). However, if there is imminent danger, the Liechtenstein Police may begin surveillance on its own initiative; but it shall forthwith report to the Prosecution Service, which shall then apply for an order to such effect from the court, unless surveillance must already be ended before. An undercover investigation pursuant to Para. (2) must be decreed by the investigating judge on application of the Prosecution Service; the investigating judge shall order the National Police to carry it out (§ 10(1)).	§ 104a § 104b § 104c

Relevant items	Provisions	Sources used
	An undercover transaction must be ordered by the investigating judge on application of the Prosecution Service, and the judge shall order the National Police to carry out the transaction (§ 8).	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	The undercover investigator shall be directed and monitored regularly by the National Police.	§ 104b
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	Code of Criminal Procedure of 18 October 1987 (StPO) (Strafprozessordnung vom 18. Oktober 1988 (StPO))	Official Language (German) 1988062000 (gesetzze.li) Unofficial English Translation https://www.legislationline.org/download/id/8270/file/Liechtenstein_Criminal_Procedure_Code_1987_am2017_en.pdf
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	Observation (Surveillance) Undercover investigation Secretly monitoring the behaviour of a person Fictitious transactions An undercover transaction in terms of this Act shall be the attempted or apparent commission of offences as far as these consist in the acquisition, obtainment, holding, import, export, or transit of items or assets that have been stolen, originate from a crime or are dedicated to committing a crime, or whose possession is absolutely prohibited.	§ 104a § 104b § 104c
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	N/A	
Specific range of application of the tool	N/A	
How is the tool defined?	N/A	
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	

Source: Author's own elaboration

Lithuania

Table 36 – Overview of national rules on investigative tools - Lithuania

Relevant items	Provisions	Sources used
Controlled Delivery		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Intelligence Law	Law on Criminal Intelligence of the Republic of Lithuania (Official Gazette, 2012, No. 122-6093). The law was published in: Žin. 2012, no. 122-6093, ik 1121010ISTA0XI-2234. 2012 October 2 No. XI-2234, Vilnius
How is the tool defined?	an authorised method of collecting information, during which goods and other objects illegally transported or suspected of being transported into or out of the territory of the Republic of Lithuania are allowed, under the control of a criminal intelligence entity, in order to clarify criminal offenses. or perpetrators.	Art 2 (5), criminal intelligence law. https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167547
For what types of crime can the tool be used?	extortion, trafficking in human beings, financial crimes, trafficking of firearms	- Art 8 (1,2,3,4), criminal intelligence law. https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167547. (Amendments to Article: No. XI-2394, 08/11/2012, Official Gazette, 2012, no. 133-6760 (2012-11-17), ik 1121010ISTA0XI-2394 - No. XII-730, 23/12/2013, published in TAR 2014-01-07, until 2014-00066 - No. XII-778, 13/03/2014, published in TAR 2014-03-27, until 2014-03569 - No. XII-2590, June 30, 2016, published in TAR 2016-07-13, until 2016-20304)
Does national law allow this tool to be used in cross border cases?	YES. Controlled delivery shall be applied only on the ground of international agreements	Art 14 (5) of criminal investigation law
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	Financial Crime Investigation Service under the Ministry of the Interior of the Republic of Lithuania, Prisons Department under the Ministry of Justice of the Republic of Lithuania, Customs Department under the Ministry of Finance of the Republic of Lithuania, Police Department under the Ministry of the Interior, Special Investigation Service, Department of Management Security, State Border Guard Service under the Ministry of the Interior of the Republic of Lithuania. The rights and duties of the main institutions of criminal intelligence also belong to the Second Department of Operational Services under the Ministry of National Defense of the Republic of Lithuania and the Department of State Security when their subdivisions conduct criminal intelligence investigations on the grounds and in accordance with this Law	Art 2 (11), criminal intelligence law. https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167547
Which LEAs can use this tool?	LEAs	Art 2 (11), criminal intelligence law. https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167547
What are the rules to be followed for the implementation of this tool?	Controlled delivery shall be sanctioned by prosecutor basing on the motivated request of the head of criminal intelligence subject or his authorised deputy. 2. The request shall contain: 1) The name, last name and position of officer who submitted the request; 2) The Data and (or) reasons justifying the necessity to carry out controlled delivery and the desired result. 3) The available data about the natural or legal person (s) who transports controlled object; 4) The names of the states from which and to which the controlled object is transported; 5) The duration of controlled delivery; 6) The desired result, as well as interim and final goals of controlled delivery. 3. After sanctioning of controlled delivery the head of criminal intelligence subject or his authorised deputy shall send (transfer) one copy of the order to general prosecutor or his authorised prosecutor of General prosecution service not later than next workday. In the case in which prosecutor refuses give the request for sanctioning of controlled delivery, the head of criminal intelligence subject or his authorised deputy has the right to apply to superior prosecutor who controls legality of criminal intelligence subject's actions. The refusal of prosecutor shall be justified in writing. The prosecutor who decided to refuse the sanctioning of indicated actions shall inform about this refusal the general prosecutor or his authorised prosecutor of General prosecution service. 4. The implementation of controlled delivery shall be forbidden in cases of danger to person's life, health or other grave consequences.	Art 14 (1), (20), (3) and (4) of criminal intelligence law. https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167547
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	1. Criminal intelligence shall not violate human rights and freedoms. Individual restrictions on these rights and freedoms are temporary and may be applied only in accordance with the procedure established by law in order to protect the rights and freedoms of another person, property, public and state security. 2. Criminal intelligence shall be carried out without regard to the sex, race, nationality, language, origin, social status, religion, belief or opinion of persons.	Art 5, 1 to 9, criminal intelligence law. https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167547

Relevant items	Provisions	Sources used
	3. It is prohibited to apply criminal intelligence to the President of the Republic. 4. It is prohibited for criminal intelligence entities to provoke persons to commit criminal offenses.	
What authorisation is needed for the use of this tool?	Controlled delivery shall be sanctioned by prosecutor based on the motivated request of the head of criminal intelligence subject or his authorised deputy.	Art 14 (1), criminal intelligence law. https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167547
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Data available on the number of times this tool has been used for SOC cases	N/A	
Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	N/A	
How is the tool defined?	N/A	
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Intelligence Law	https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167547
How is the tool defined?	The national law does not clearly defines this tool, but broadly explains/provides some general information which is - "to persons involved in criminal proceedings: witnesses, victims, experts, professionals and advocates (representatives), legal representatives, suspects, accused, convicted, acquitted persons to whom pre-trial investigation is terminated".	Art. 4 (1) of Criminal intelligence law
For what types of crime can the tool be used?	extortion, trafficking in human beings, financial crimes, trafficking of firearms	- Art 5, 1 to 9, criminal intelligence law. https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167547. - Art 8 (1,2,3,4), criminal intelligence law. https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167547. (Amendments to Article: - No. XI-2394 , 08/11/2012, Officia Gazzette, 2012, no. 133-6760 (2012-11-17), ik 1121010ISTA0XI-2394 - No. XII-730 , 23/12/2013, published in TAR 2014-01-07, until 2014-00066 - No. XII-778 , 13/03/2014, published in TAR 2014-03-27, until 2014-03569 - No. XII-2590 , June 30, 2016, published in TAR 2016-07-13, until 2016-20304)

Relevant items	Provisions	Sources used
Does national law allow this tool to be used in cross border cases?	Lithuanian Criminal Police Bureau - This is a specialised police agency established on a non-territorial basis. It aims at preventing and investigating serious crimes and comprises the following investigating units: Organised Crime Investigation Board 1-2-3; Cyber Crime Investigation Board; Asset Recovery Board; Serious Crime Investigation Board; Pre-trial Investigation Board. The following special assignments units: Special Assignments Board 1- 2-3; International Liaison Office. Two management and control units: Activity Coordination and Control Board; Information Technology Board (works for national and international area) General Prosecution Service -This institution comprises prosecutors and special divisions focusing on organised crime. Among other things it plays a very important role in coordinating pre-trial investigations. It also contributes to the legislative process. Plays the role of the central institution in communicating with foreign institutions and international organisations. Maintains contacts and representatives at Europol, OLAF, Eurojust and at the European Judicial Network Division of Fight against Organised Crime- A special division part of the Prosecutor's General Office focusing on organised crime and corruption cases.	Page 536 of AMOC profile. Link https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/20150312_1_amoc_report_020315_0_220_part_2_en.pdf
What thresholds must be passed for the use of this tool?	General Prosecution Service -This institution comprises prosecutors and special divisions focusing on organised crime. Among other things it plays a very important role in coordinating pre-trial investigations. It also contributes to the legislative process. Plays the role of the central institution in communicating with foreign institutions and international organisations. Maintains contacts and representatives at Europol, OLAF, Eurojust and at the European Judicial Network	Page 536 of AMOC profile. Link https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/20150312_1_amoc_report_020315_0_220_part_2_en.pdf
What types of stakeholder are involved in the implementation of this tool?	The task of a law enforcement authority shall be sanctioned by a reasoned order of the presidents of the district courts or their authorised judges on the basis of motivated submissions of the prosecutor prepared on the basis of data provided by heads of criminal intelligence to collect information on the objects of criminal intelligence by participating in the activities of a criminal association or organised group and in the criminal acts committed by them in order to identify and prosecute the persons organizing and carrying out criminal acts.	Art. 12 (1) of criminal intelligence law
Which LEAs can use this tool?	1. Criminal intelligence shall not violate human rights and freedoms. Individual restrictions on these rights and freedoms are temporary and may be applied only in accordance with the procedure established by law in order to protect the rights and freedoms of another person, property, public and state security. 2. Criminal intelligence shall be carried out without regard to the sex, race, nationality, language, origin, social status, religion, belief or opinion of persons. 3. It is prohibited to apply criminal intelligence to the President of the Republic. 4. It is prohibited for criminal intelligence entities to provoke persons to commit criminal offenses.	Art 5, 1 to 9, criminal intelligence law. https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167547
What are the rules to be followed for the implementation of this tool?	The investigating judge	Art 4 (1) criminal intelligence law. https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167547
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	Criminal Intelligence Law	https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167547
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	The national law does not clearly defines this tool, but broadly explains/provides some general information which is - "to persons involved in criminal proceedings: witnesses, victims, experts, professionals and advocates (representatives), legal representatives, suspects, accused, convicted, acquitted persons to whom pre-trial investigation is terminated".	Art. 4 (1) of Criminal intelligence law
Surveillance		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Procedure Code	https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.163482/asr
Specific range of application of the tool	It is mostly used with covert surveillance. Including Audio and Video Surveillance.	Article 160 (2), Criminal Procedure code. Link - https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.163482/asr
How is the tool defined?	The pre-trial judge may, at the request of the prosecutor, order the tracking of a person or vehicle or object. The order of the pre-trial investigation judge, the decision of the pre-trial investigation officer or the prosecutor to order the tracking of a person or a vehicle or object	Article 160 (1), Criminal Procedure code. Link - https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.163482/asr

Relevant items	Provisions	Sources used
For what types of crime can the tool be used?	extortion, trafficking in human beings, financial crimes, trafficking of firearms	- Art 5, 1 to 9, criminal intelligence law. https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167547. Art 8 (1,2,3,4), criminal intelligence law. https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167547. (Amendments to Article: - No. XI-2394 , 08/11/2012, Officia Gazzette, 2012, no. 133-6760 (2012-11-17), ik 1121010ISTA0XI-2394 - No. XII-730 , 23/12/2013, published in TAR 2014-01-07, until 2014-00066 - No. XII-778 , 13/03/2014, published in TAR 2014-03-27, until 2014-03569 - No. XII-2590 , June 30, 2016, published in TAR 2016-07-13, until 2016-20304)
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	1) upon receipt of a complaint, statement or notification regarding a criminal offense; 2) if the prosecutor or the pre-trial investigation officer has established the signs of the criminal offense. 2 . In the cases provided for in this Code, the pre-trial investigation shall be initiated only in the event of a complaint by the victim. 3 . Each case of the commencement of a pre-trial investigation shall be registered in accordance with the procedure established by the Prosecutor General of the Republic of Lithuania. 4 . The person who submitted the complaint, statement or notification shall be notified of the commencement of the pre-trial investigation.	Art 166 (1), (2), (3) and (4). criminal intelligence law. https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167547. No. XIII-626 , 2017-07-11, published in TAR 2017-07-24, to 2017-12575
What types of stakeholder are involved in the implementation of this tool?	Pre-trial investigation institutions also include the regular police, State Border Guard Service, the Special Investigation Service, the Military Police, the Financial Crime Investigation Service, the Customs of the Republic of Lithuania, the Fire and Rescue Department when investigating criminal acts revealed by these institutions	Art 165 (1), code of criminal procedure https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.163482/asr
Which LEAs can use this tool?	The pre-trial investigation is carried out by pre-trial investigation officers. The pre-trial investigation is organised and directed by the prosecutor. The prosecutor may decide to conduct all or part of the pre-trial investigation himself.	Art 165 (1), criminal intelligence law. https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167547
What are the rules to be followed for the implementation of this tool?	The surveillance report and other documents related to the surveillance shall be drawn up in accordance with the rules laid down in Article 201 of this Code. The covert surveillance protocol shall contain only data relevant to the investigation. Data not relevant to the investigation, which are not in a common medium with data relevant to the case, shall not be attached to the case and shall be immediately destroyed by a resolution of the prosecutor upon drawing up the relevant act. An officer who has carried out undercover surveillance may be questioned as a witness. The interrogation may be conducted in accordance with Articles 203 and 282 of this Code, and the identification and confrontation may be conducted in accordance with the rules set out in Article 204 of this Code. With the written consent of the intelligence officer, the intelligence record may be drawn up in accordance with the general rules on the conduct and recording of investigations laid down in Article 179 of this Code, and the intelligence officer may be questioned as a witness in accordance with rules	Article 160 (3), (4), (5). Criminal Procedure code. Link - https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.163482/asr
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	1. Criminal intelligence shall not violate human rights and freedoms. Individual restrictions on these rights and freedoms are temporary and may be applied only in accordance with the procedure established by law in order to protect the rights and freedoms of another person, property, public and state security. 2. Criminal intelligence shall be carried out without regard to the sex, race, nationality, language, origin, social status, religion, belief or opinion of persons. 3. It is prohibited to apply criminal intelligence to the President of the Republic. 4. It is prohibited for criminal intelligence entities to provoke persons to commit criminal offenses.	Art 5, 1 to 9, criminal intelligence law. https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167547
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Only the prosecutor makes decisions- 1) on the aggregation and separation of research; 2) regarding the suspension of the pre-trial investigation; 3) regarding the termination of the pre-trial investigation, except in the cases provided for in Paragraph 1 of Article 214 of this Code ; 4) due to the resumption of the terminated pre-trial investigation; 5) regarding the completion of the investigation and the drawing up of the indictment.	Article 170-4, 1,2,3,4, 5. Criminal Procedure code. Link - https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.163482/asr
What ongoing supervision is required for the use of this tool?	Surveillance shall be authorised by the prosecutor on the motivated submission of the head of the criminal intelligence entity or the deputy head of the authorised intelligence unit.	Art. 15 (2), Criminal Intelligence Law. https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167547
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime	N/A	

Relevant items	Provisions	Sources used
cases? If yes can you please indicate the relevant statistics?		
Undercover / covert operations		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Procedure Code	https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.111555/asr
How is the tool defined?	The actions of pre-trial investigation officers who do not reveal their identity are allowed by the order of the pre-trial investigation judge and only if there are sufficient data on the crime of the person under investigation	Art 158 (2), Criminal intelligence law. https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167547
For what types of crime can the tool be used?	A prosecutor who has received information from a person that that person is being offered to commit or participate in the commission of a crime may apply to the pre-trial judge with a request to allow that person to perform acts imitating a criminal offense in order to identify the perpetrators	Art 159 (1), Criminal intelligence law. https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167547
Does national law allow this tool to be used in cross border cases?	a method of gathering criminal intelligence information, when secret participants of criminal intelligence, as well as employees of criminal intelligence subjects are used or otherwise used in the framework of a criminal intelligence investigation. The procedure for conducting covert operations shall be established by the main criminal intelligence authorities.	Art. 2 (18), Criminal intelligence law. https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167547
What thresholds must be passed for the use of this tool?	extortion, trafficking in human beings, financial crimes, trafficking of firearms	- Art 5, 1 to 9, criminal intelligence law. https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167547. - Art 8 (1,2,3,4), criminal intelligence law. https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167547. (Amendments to Article: No. XI-2394 , 08/11/2012, Officia Gazzette, 2012, no. 133-6760 (2012-11-17), ik 1121010ISTA0XI-2394 - No. XII-730 , 23/12/2013, published in TAR 2014-01-07, until 2014-00066 - No. XII-778 , 13/03/2014, published in TAR 2014-03-27, until 2014-03569 - No. XII-2590 , June 30, 2016, published in TAR 2016-07-13, until 2016-20304)
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	Only the prosecutor makes decisions- 1) on the aggregation and separation of research; 2) regarding the suspension of the pre-trial investigation; 3) regarding the termination of the pre-trial investigation, except in the cases provided for in Paragraph 1 of Article 214 of this Code ; 4) due to the resumption of the terminated pre-trial investigation; 5) regarding the completion of the investigation and the drawing up of the indictment.	Article 170-4, 1,2,3,4, 5. Criminal Procedure code. Link - https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.163482/asr
What are the rules to be followed for the implementation of this tool?	The institution of pre-trial investigation is the police. Pre-trial investigation institutions also include the State Border Guard Service, the Special Investigation Service, the Military Police, the Financial Crime Investigation Service, the Customs of the Republic of Lithuania, the Fire and Rescue Department when investigating criminal acts revealed by these institutions . 2 . The pre-trial investigation shall also be carried out by the masters of long-distance seagoing vessels - officers of the Department of Prisons, directors of detention, pre-trial detention and correctional facilities or their authorised officers - in respect of crimes committed by crew members and passengers during long-distance voyages.	Art 165 (1) and (2), criminal intelligence law. https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167547
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	1 . The pre-trial investigation is carried out by pre-trial investigation officers. The pre-trial investigation is organised and directed by the prosecutor. The prosecutor may decide to conduct all or part of the pre-trial investigation himself. 2 . In the cases provided for in this Code, certain actions of the pre-trial investigation shall be performed by the pre-trial investigation judge.	Art 164 (1), (2). Criminal intelligence law. https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167547
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	When the pre-trial investigation or individual actions thereof are carried out by pre-trial investigation officers, the prosecutor must monitor the conduct of the pre-trial investigation.	Art 170 (2). Criminal intelligence law. https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167547
What ongoing supervision is required for the use of this tool?	Only the prosecutor makes decisions: 1) on the aggregation and separation of research; 2) regarding the suspension of the pre-trial investigation; 3) regarding the termination of the pre-trial investigation, except in the cases provided for in Paragraph 1 of Article 214 of this Code ; 4) due to the resumption of the terminated pre-trial investigation; 5) regarding the completion of the investigation and the drawing up of the indictment	Art 170-4, 1,2,3 and 4. Code of Criminal code. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.163482/asr
Is there any national case law relating to the use of this tool in cross-border crime cases?	1. Criminal intelligence shall not violate human rights and freedoms. Individual restrictions on these rights and freedoms are temporary and may be applied only in accordance with the procedure established by law in order to protect the rights and freedoms of another person, property, public and state security.	Art 5, 1 to 9, criminal intelligence law. https://www.lrs.lt/sip/portal.show?p_r=36483&p_k=1&p_t=167547

Relevant items	Provisions	Sources used
	2. Criminal intelligence shall be carried out without regard to the sex, race, nationality, language, origin, social status, religion, belief or opinion of persons. 3. It is prohibited to apply criminal intelligence to the President of the Republic. 4. It is prohibited for criminal intelligence entities to provoke persons to commit criminal offenses.	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	The Prosecution	Art 170-4. Code of Criminal code. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.163482/asr
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	N/A	
Specific range of application of the tool	N/A	
How is the tool defined?	N/A	
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	

Source: Author’s own elaboration

Luxembourg

Table 37 – Overview of national rules on investigative tools - Luxembourg

Relevant items	Provisions	Sources used
Controlled Delivery		
Relevant documents (legal and non-legal) that define the functioning of the tool	N/A	
How is the tool defined?	N/A	
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross border cases?	N/A	

Relevant items	Provisions	Sources used
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Data available on the number of times this tool has been used for SOC cases	N/A	
Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	N/A	
How is the tool defined?	N/A	
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	N/A	
How is the tool defined?	N/A	
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross border cases?	N/A	

Relevant items	Provisions	Sources used
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Surveillance		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Instruction Code	https://www.legislationline.org/searchn2/runSearch/1/key/Criminal+instruction+code+of+luxembourg/country/16/rows/10/type/-1,0,0,0,0
Specific range of application of the tool	video camera and audio	Art 48-12 (1) Art 48-12 para 3
How is the tool defined?	The systematic observation using audio, video tools, of one or more persons suspected performing criminal activity.	Art 48-12 (1)
For what types of crime can the tool be used?	Does not say about any specific crime within the tool, but usually says that according to Articles 479, 480 and 481 of the Penal Code this act will enforced	Art 48-13 (3)
Does national law allow this tool to be used in cross border cases?	No information found in the national law	Previous study confirms this finding
What thresholds must be passed for the use of this tool?	No specific information found in the law.	Previous study confirms this finding
What types of stakeholder are involved in the implementation of this tool?	the investigative judge or the public prosecutor	Art 48-12 (1), and (2)
Which LEAs can use this tool?	LEAs and Judicial Police	- Art. 48-13 §2 - Art 48-14 (1) - 1,2,3
What are the rules to be followed for the implementation of this tool?	The following procedure has to follow: - (1) The determination of the procedure for the State or the instruction of the procedure for observing the procedure is written and maintained, under nullity, the following comments: the serious indication of the offense referred to in subsections (2) or (3) of article 48-13 and which justify the observation; 2 ° the specific motives for the instructions or preparation instruction followed by an observation; 3 ° the name or, if it is not known, a description also specify as possible of the person (s) observed, in addition to what is required, of the events or events referred to in Article 48-12, paragraph (1); 4 ° manner in which the observation will be carried out, including permission to use technical means in the cases provided for in article 48-13, paragraphs (2) and (3). In the case of Article 48-13, para (3), the specification of the instruction mention the address or location precisely that is possible of habitation which is the object of observation;	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Any decision of the public prosecutor or the investigative judge which authorizes surveillance measures must be duly justified . Under penalty of nullity, it shall mention the existing evidence indicates that an offence has been committed, specific reasons for the need of surveillance, the targeted person of place, how surveillance will be undertaken, its duration, as well as the competent police officer.	Art. 48-14
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	investigative judge	Art. 48-13 §3
What ongoing supervision is required for the use of this tool?	N/A	

Relevant items	Provisions	Sources used
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Undercover / covert operations		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Instruction Code	https://www.legislationline.org/searchn2/runSearch/1/key/Criminal+instruction+code+of+luxembourg/country/16/rows/10/type/-1,0,0,0,0
How is the tool defined?	Art 48-17 (1) allows undercover investigations in respect of both criminal association and criminal organisation when related to a list of serious offences, including arms trafficking, murder or grievous bodily injury, robbery and extortion, corruption, money laundering, drug trafficking and trafficking in human beings	Art 48-17 (1)
For what types of crime can the tool be used?	serious offences, including arms trafficking, murder or grievous bodily injury, robbery and extortion, corruption, money laundering, drug trafficking and trafficking in human beings	Art. 48-17§1
Does national law allow this tool to be used in cross border cases?	YES. Judicial police officers can help other states police in authorised/permitted undercover operation.	Art 48-19 (1)
What thresholds must be passed for the use of this tool?	No information found in the national law	Previous study confirms this finding
What types of stakeholder are involved in the implementation of this tool?	Judicial authority, LEAs	Art. 48-17§1
Which LEAs can use this tool?	LEAs and Judicial Police	Art 48-19 (1)
What are the rules to be followed for the implementation of this tool?	1) Upon the request of state police judicial police can ask for permission for covert operations. The decision has to be duly justified by referring to strong evidence that one of the above mentioned offences has been committed, specific reasons for the need of a covert investigation, its length that may not exceed four month, the competent police office. 2) The duration may be extended for four additional months if duly justified. 3) Police officers may carry out the covert operation without incurring any criminal liability	1) Art. 48-18§1 2) Art. 48-18§2 3) Art. 48-19
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	1) covert investigations cannot be conducted in respect of the accused after his first interrogation by the investigative judge 2) the undercover officer shall not induce a person to commit an offence (agent provocateur) either by exercising any moral or material pressure or by interfering in the overall design and planning of the offence	1) Art. 48-17§2 2) C.S.J., corr., 25 March 1988. See also R. Nothar, La charge de la preuve en droit pénal, Bull. Laurent, 1990-I, pp. 35 et seq. ; J.Petry, Droit pénal – Procédure pénale. Jurisprudence récente, Pas. XXXI, pp. 97 et seq
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Judicial Police	Art 48-22 (1)
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	N/A	
Specific range of application of the tool	N/A	
How is the tool defined?	N/A	
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	N/A	

Relevant items	Provisions	Sources used
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	

Source: Author’s own elaboration

Malta

Table 38 – Overview of national rules on investigative tools - Malta

Relevant items	Provisions	Sources used
Controlled Delivery		
Relevant documents (legal and non-legal) that define the functioning of the tool	<u>Dangerous Drugs Ordinance Chapter 101</u> Article 30B.(1) Notwithstanding anything contained in any other law, it shall be lawful for the Executive Police and, where appropriate, the Customs Authorities to allow, with the consent of the Attorney General or of a magistrate, a controlled delivery to take place. (2) For the purposes of this article a controlled delivery means the technique of allowing an illicit or suspect consignment of a dangerous drug (as defined in article 12) or of money, property or proceeds as referred to in article 22(1C)(a) to pass out of, through or into Malta, or from one place or person in Malta to another place or person in Malta, or into the territory of another country, with the knowledge and under the supervision of the Executive Police and, where appropriate, of the Customs Authorities and of the competent authorities of such other country, with a view to identifying persons involved in commission of offences under this Ordinance or under the corresponding law in force in the territory of such other country. <u>Criminal Code Chapter 9 Article 435E</u> .435E. (1) Notwithstanding anything contained in any other law it shall be lawful for the Attorney General to authorise the Executive Police and, where appropriate, the Customs authorities to allow a controlled delivery to take place with a view to identifying persons involved in the commission of any criminal offence under the laws of Malta or under the laws of another country. For the purposes of this sub-article a "controlled delivery" shall mutatis mutandis have the same meaning assigned to it by article 30B(2) of the Dangerous Drugs Ordinance so however that the illicit or suspect consignment referred to in that sub-article may for the purposes of this sub-article consist of anything what so ever and that the consignment may be intercepted and allowed to continue with the original contents intact or removed or replaced in whole or in part. (2) With the same objective of identifying persons involved in the commissions of a criminal offence under the laws of Malta or under the laws of another country, it shall also be lawful for the Attorney General to authorise the Executive Police or a person under the supervision or direction of the Executive Police, to acquire or procure an illicit or suspect consignment of anything from any person or place. (3) Pursuant to any arrangement, including any treaty ,convention, agreement or understanding, to which Malta is a party or which is otherwise applicable to Malta, the Attorney General may authorise the competent authorities of another country to conduct in Malta, jointly with or under the supervision or direction of the Executive Police, investigations into criminal offences by officers acting under covert or false identity, provided that the Attorney General is satisfied of the true identity and official capacity of the officers in question and is fully informed of the nature of any documents which purport to guarantee, certify or authenticate the false identity assumed by any such officers Notwithstanding the provisions of any other law the making or use of such documents by the said competent authorities or by such officers for the purpose or in the course	• Dangerous Drugs Ordinance Chapter 101 Article 30B • Criminal Code Chapter 9 Article 435E • https://www.fatf-gafi.org/media/fatf/documents/reports/mer-fsrb/Moneyval-Mutual-Evaluation-Report-Malta-2019.pdf

Relevant items	Provisions	Sources used
	of such investigations authorised as aforesaid shall be deemed to be lawful and shall not entail any liability, civil, criminal or otherwise, on the part of such authorities or officers. (4) Any official from another country taking part in any of the operations referred to in sub-articles (1) to (3), both inclusive, shall, for the purpose of any criminal liability incurred under this Code or any other law by that official or by others for conduct against that official, be deemed to be a public officer. (5) The provisions of sub-article (4) shall apply mutatis mutandis to any official from another country taking part in an operation in Malta of the kind referred to in sub-article (3) even if none of the officers taking part in the operation is acting under covert or false identity. Cap. 460.(6) For purposes of this article "competent authorities of another country" and "official from another country" shall be construed as including officials of bodies set up pursuant to the Treaty on European Union as defined in article 2 of the European Union Act. (7) Where the Attorney General has authorised the setting up of a joint investigation team as provided in sub-article (3), the foreign officials participating in the said investigation shall be entitled to be present when investigative measures are being taken and, if so authorised by the competent officer of the Executive Police, to take investigative measures. <u>Anti-money laundering and counter-terrorist financing measures - Fifth Round Mutual Evaluation Report July 2019</u> Malta's competent authorities are empowered to use a wide range of investigative techniques for the investigation of ML, associated predicate offences and FT, such as undercover operations (Art. 435E (3) CC), accessing computer systems (Art. 355P and 355Q CC) and controlled deliveries	
How is the tool defined?	In the Dangerous Drugs Ordinance Article 30B (2) 'a controlled delivery means the technique of allowing an illicit or suspect consignment of a dangerous drug (as defined in article 12) or of money, property or proceeds as referred to in article 22(1C)(a) to pass out of, through or into Malta, or from one place or person in Malta to another place or person in Malta, or into the territory of another country, with the knowledge and under the supervision of the Executive Police and, where appropriate, of the Customs Authorities and of the competent authorities of such other country, with a view to identifying persons involved in commission of offences under this Ordinance or under the corresponding law in force in the territory of such other country'	Dangerous Drugs Ordinance Chapter 101 Article 30B
For what types of crime can the tool be used?	Organised crime, Drugs, money and property.	- Dangerous Drugs Ordinance Chapter 101 Article 30B - Criminal Code Chapter 9 Article 435E https://www.fatf-gafi.org/media/fatf/documents/reports/mer-fsrb/Moneyval-Mutual-Evaluation-Report-Malta-2019.pdf
Does national law allow this tool to be used in cross border cases?	There is no specific law that stipulates cross-border cases, however according to the Criminal Code, "Notwithstanding anything contained in any other law it shall be lawful for the Attorney General to authorise the Executive Police and, where appropriate, the Customs authorities to allow a controlled delivery to take place with a view to identifying persons involved in the commission of any criminal offence under the laws of Malta or under the laws of another country."	Chapter 9 Criminal Code Article 435E (1)
What thresholds must be passed for the use of this tool?	Controlled Delivery in Malta can be used for any criminal offence under the laws of Malta or of another country.	Chapter 9 Criminal Code Article 435E (1)
What types of stakeholder are involved in the implementation of this tool?	LEAs (Executive Police and Customs), and other competent authorities from abroad. As per the Criminal Code Chapter 9 , "competent authorities of another country" and "official from another country" shall be construed as including officials of bodies set up pursuant to the Treaty on European Union as defined in article 2 of the European Union Act. LEA role is to investigate further into criminal offences, where the executive police may acquire or procure an illicit or suspect consignment of anything from any person or place.	Chapter 9 Criminal Code Article 435E (2) (3) (6)
Which LEAs can use this tool?	Police and Customs authorities, only if authorised by the Attorney General	Chapter 9 Criminal Code Article 435E (1)
What are the rules to be followed for the implementation of this tool?	1. If any other official from any other country is taking part in a controlled delivery, he/she shall be deemed to be a public officer. The law does not mention cross- border crime cases. 2. Authorisation is always needed to be able to conduct a controlled delivery. There is no reference in the law and no desktop research available in relation to rules which are required when executive police and customs implement this tool.	Chapter 9 Criminal Code Article 435E (4)
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	This has not been specifically stipulated in the law and no evidence from desktop research could be identified in this regard.	
What authorisation is needed for the use of this tool?	In order for this tool to be implemented, an authorisation form the Attorney General or Magistrate is needed. There is no specific law that stipulates the process of obtaining this authorisation.	- Chapter 9 Criminal Code Article 435E (1) - Dangerous Drugs Ordinance Chapter 101 Article 30B
What ongoing supervision is required for the use of this tool?	Ongoing supervision is required by the Executive police and in some instances Customs authorities. The law does not go into the detail of the requirements.	- Chapter 9 Criminal Code Article 435E (2)(3) - Dangerous Drugs Ordinance Chapter 101 Article 30B

Relevant items	Provisions	Sources used
Is there any national case law relating to the use of this tool in cross-border crime cases?	No desktop research available	
Data available on the number of times this tool has been used for SOC cases	No recent statistics available, however through desktop research we could only identify the following two scenarios; 1)According to the Ministry of Home Affairs and security's Annual report of 2013, the drug squad managed to conclude various drug related investigations, using controlled-delivery. 2)In 2018, 100 kg of cocaine were detected, in February, with the scanner in a container at the Freeport, but sent under a controlled delivery procedure to Croatia, where a huge criminal gang was arrested. (Dwana press release 2018)	https://www.gov.mt/en/Government/Government%20of%20Malta/Ministries%20and%20Entities/Annual%20Government%20Reports/Documents/Annual%20Reports%202013/MHAS.pdf https://ec.europa.eu/anti-fraud/sites/antifraud/files/09012019_malta_customs_narcotics_seizures_en.pdf
Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	<u>Chapter 226 Article.8.</u>(1) Nothing in this Act shall be construed as affecting any jurisdiction and power exercisable in accordance with international law outside territorial waters, and in particular the following provisions of this article shall apply. (2) Subject to the provisions of sub article (3), where a relevant vessel or craft has, within Maltese internal or territorial waters, or within the contiguous zone of Malta, commenced the pursuit of a suspect vessel, the relevant vessel may continue in hot pursuit of the suspect vessel into the high seas provided that the pursuit has not been interrupted: Provided that where the suspect vessel is within the contiguous zone when it is ordered to stop by a maritime enforcement officer on board the relevant vessel, the pursuit may only be undertaken if the suspect vessel is suspected of having committed any relevant offence. (3) Where the suspect vessel is within the contiguous zone, hot pursuit may only be undertaken if the commission of a relevant offence is reasonably suspected. (4) The right of hot pursuit referred to in this article shall not be undertaken unless the relevant vessel or craft has first given the suspect vessel a visual or auditory signal to stop and the said right of hot pursuit shall cease where the suspect vessel enters the territorial sea of its own State or of a third State. (5) Where hot pursuit is effected by an aircraft the provisions of sub articles (2) to (4) shall apply mutatis mutandis. The provisions of sub article (6) shall also apply. (6) An aircraft shall not arrest a suspect vessel outside the territorial waters of Malta unless the aircraft had itself ordered the suspect vessel to stop and had pursued it without interruption, and where hot pursuit had been undertaken by an aircraft and the pursuit was taken over by another aircraft or ship, such other aircraft or ship shall only be authorised to arrest the suspect vessel outside the territorial waters of Malta if the said other aircraft or ship had continued the pursuit without interruption. (7) The right of hot pursuit shall apply mutatis mutandis to any violation in the area established by article 3(2) or of any law for the purposes of which the said area is established. (8) Where a Maltese military vessel encounters on the high seas a foreign vessel, not being a foreign military vessel or a ship owned by a foreign State used only on non-commercial service ,hereafter referred to in this sub article as the suspect vessel, and there is reasonable ground for suspecting that -(a) the suspect vessel is engaged in piracy;(b) the suspect vessel is engaged in the slave trade;(c) the suspect vessel is engaged in unauthorised broadcasting and the Maltese courts have jurisdiction hereon;(d) the suspect vessel is without nationality; or(e) though flying a foreign flag or refuses to show its flag, the suspect vessel is a vessel registered in Malta, any maritime enforcement officer on board the relevant vessel may proceed to verify the suspect vessel's right to fly its flag by boarding the suspect vessel and checking its documents and if there upon suspicion remains as to the nationality of the suspect vessel, the relevant vessel may proceed to a further examination with all possible consideration. (9) Any person or suspect vessel discovered to be engaged in unauthorised broadcasting as provided in sub article (7)(c) may be arrested by any maritime enforcement officer on board the relevant vessel who may also seize any apparatus used in the said unauthorised broadcasting As per Chapter 226 Article 4 (2) the contiguous zone shall; Extend to twenty-four nautical miles from the baselines from which the breadth of the territorial waters is measured.	Chapter 226 Article 8/4 – Terrestrial waters and Contiguous zone act
How is the tool defined?	N/A	N/A
For what types of crime can the tool be used?	Hot pursuit is used for any 'relevant offences' which according to Chapter 226, such offences include, customs, fiscal matters, immigration and sanitation, including pollution.	Chapter 226 Article 8 (1) – Terrestrial waters and Contiguous zone act
Does national law allow this tool to be used in cross border cases?	No	Manual of Cross-border operations - EU Council 2017 - https://www.statewatch.org/media/documents/news/2017/sep/eu-council-manual-cross-border-ops-11840-17.pdf
What thresholds must be passed for the use of this tool?	<u>Chapter 226 Article 8</u> states :(2) Subject to the provisions of sub article (3), where a relevant vessel or craft has, within Maltese internal or territorial waters, or within the contiguous zone of	Chapter 226 Article 8 (2) (3) – Terrestrial waters and Contiguous zone act

Relevant items	Provisions	Sources used
	Malta, commenced the pursuit of a suspect vessel, the relevant vessel may continue in hot pursuit of the suspect vessel into the high seas provided that the pursuit has not been interrupted; Provided that where the suspect vessel is within the contiguous zone when it is ordered to stop by a maritime enforcement officer on board the relevant vessel, the pursuit may only be undertaken if the suspect vessel is suspected of having committed any relevant offence.(3) Where the suspect vessel is within the contiguous zone, hot pursuit may only be undertaken if the commission of a relevant offence is reasonably suspected The law does not clarify what constitutes an 'interruption'.	
What types of stakeholder are involved in the implementation of this tool?	LEAs	
Which LEAs can use this tool?	LEAs such as Armed Forces of Malta, the Police Force and Customs officers. According to Chapter 226, "maritime enforcement officer" means any member of the Malta Police Force, of the Armed Forces of Malta, any Customs Officer and any other officer vested with general law enforcement authority' There is no distinction within the law on the requirements/authorisations required by specific LEAs.	Chapter 226– Terrestrial waters and Contiguous zone act
What are the rules to be followed for the implementation of this tool?	(4) The right of hot pursuit referred to in this article shall not be undertaken unless the relevant vessel or craft has first given the suspect vessel a visual or auditory signal to stop and the said right of hot pursuit shall cease where the suspect vessel enters the territorial sea of its own State or of a third State 8) Where a Maltese military vessel encounters on the high seas a foreign vessel, not being a foreign military vessel or a ship owned by a foreign State used only on non-commercial service, hereafter referred to in this sub article as the suspect vessel, and there is reasonable ground for suspecting that -(a) the suspect vessel is engaged in piracy;(b) the suspect vessel is engaged in the slave trade;(c) the suspect vessel is engaged in unauthorised broadcasting and the Maltese courts have jurisdiction thereon;(d) the suspect vessel is without nationality; or(e) though flying a foreign flag or refuses to show its flag, the suspect vessel is a vessel registered in Malta, any maritime enforcement officer on board the relevant vessel may proceed to verify the suspect vessel's right to fly its flag by boarding the suspect vessel and checking its documents and if thereupon suspicion remains as to the nationality of the suspect vessel, the relevant vessel may proceed to a further examination with all possible consideration.	Chapter 226 Article 8 (4) (8) – Terrestrial waters and Contiguous zone act
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	No authorisation needed, apart from that is given by the maritime enforcement officer. 6.(1) Any maritime enforcement officer on board a relevant vessel or craft may, within the contiguous zone, take appropriate action with respect to any vessel, other than a foreign military vessel or a ship owned by a foreign state used only for non-commercial service, whether flying the Maltese or any other flag or not flying any flag, reasonably suspected of having on board any person reasonably suspected of being about to commit or of having committed within the jurisdiction of the Maltese courts any relevant offence	Chapter 226 Article 6 (1)– Terrestrial waters and Contiguous zone act
What ongoing supervision is required for the use of this tool?	Article 5(3) The provisions of sub article (2) shall not affect the right of any maritime enforcement officer on board any relevant vessel or craft to take any steps authorised by Maltese law for the purpose of an arrest or investigation on board a foreign vessel passing through the territorial waters of Malta after leaving Maltese internal waters. In the definition, any instrument having the force of law is included.	Chapter 226 Article 5 (3)– Terrestrial waters and Contiguous zone act
Is there any national case law relating to the use of this tool in cross-border crime cases?	None. Malta is surrounded by high seas and has no land borders with any of the participating States. (hot pursuit under Article 41 of the Schengen Convention is not applicable.)	Manual of Cross-border operations - EU Council 2017 - https://www.statewatch.org/media/documents/news/2017/sep/eu-council-manual-cross-border-ops-11840-17.pdf
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	40.(1) Where a person who is the victim of a crime is to be produced as a witness in any criminal proceedings against any principal or accomplice in the crime and that person is concerned for his safety or there exist concerns over that person's safety, the Commissioner may, subject to the provisions of article 39, set up a witness protection programme hereinafter referred to in this Part as "the programme". (2) The provisions of sub-article (1) shall also apply to a person who took part in the commission of a crime and whose evidence is required for the prosecution of any principal or accomplice in	Chapter 164 Police Act Article 40. (May 2017)

Relevant items	Provisions	Sources used
	the crime where that person agrees to co-operate with the public authorities for the purpose of such prosecution. 41.A person may become entitled to benefit under the programme if that person -(a) is a victim of a crime; or(b) participated in any organisation or group of persons who have committed or are organised to commit any crime; or(c) has participated in the commission of a crime liable to the punishment of imprisonment of seven years or more, and, where paragraph (b) or (c) applies, reveals to the Police such information which the Police consider sufficient as to be likely to secure, upon an eventual prosecution, the conviction of other participants in the crime. 42.With respect to a person entitled to be admitted to the programme under article 41(b) or (c) the programme shall only apply if that person declares that he will testify during any trial of any participant in the crime and any benefit granted shall be forfeited if the witness refuses to so testify	
How is the tool defined?	40.(1) Where a person who is the victim of a crime is to be produced as a witness in any criminal proceedings against any principal or accomplice in the crime and that person is concerned for his safety or there exist concerns over that person's safety, the Commissioner may, subject to the provisions of article 39, set up a witness protection programme hereinafter referred to in this Part as "the programme".	Chapter 164 Police Act Article 40
For what types of crime can the tool be used?	Chapter 164 Article 40 states that it is used in any criminal proceeding, however it is not specified.	Chapter 164 Police Act Article 40,41,44
Does national law allow this tool to be used in cross border cases?	49.The Minister responsible for the Police may enter into agreements with foreign governments providing for assistance, on the basis of reciprocity, in the implementation of witness protection programmes. For the purpose of enhancing the protection of witnesses such agreements may provide for the possibility of transferring to another country a protected witness or receiving from another country a witness admitted to a programme in that country	Chapter 164 Police Act Article 49
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	Judicial authorities and LEA	Chapter 164 Police Act Title II
Which LEAs can use this tool?	Police Authorities	- Chapter 164 Police Act - Chapter 164 Police Act Art 43 (2)
What are the rules to be followed for the implementation of this tool?	2) The Minister, with the concurrence of the Minister responsible for Justice, may make regulations to provide for the modalities, conditions and rules of procedure to be applied when a person is to give evidence under the provisions of sub-article (1). Rules are not specified in the Act and could not be identified through desktop research.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	48.The programme may provide for such protection to the life and property of a witness admitted to the programme and to that of members of his family in the ascending, descending or collateral line, as the Commissioner may deem appropriate and may include provision for the payment of a subsistence allowance in particular cases	Chapter 164 Police Act Art 48
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	The commissioner of the Police has to set up the witness protection programme	Chapter 164 Police Act Article 40
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Surveillance		
Relevant documents (legal and non-legal) that define the functioning of the tool	No legislation in this regard. However, it is mentioned in several Acts such as In Chapter 391 Security Service Act, Chapter 226 - Terrestrial waters and contiguous zone act and in the Processing of Personal Data Subsidiary legislation (SL 586). In Chapter 391 Surveillance is mentioned under "interception", in relation to a warrant, includes the obtaining possession of, disrupting, destroying, opening, interrupting, suppressing, stopping, seizing, eavesdropping on, surveillant, recording, copying, listening to and viewing of communications and the extraction of information from such communications. Article 6 states that (2) No interception of or interference with communications in the course of their transmission by post or by means of a radiocommunications or telecommunication system or by any other means shall be unlawful if it is authorised by a warrant issued by the Minister under this article. Further, Article 7 talks about warrants with regards to interceptions ;7.(1) Subject to sub article (2), the interception or interference with communications required by a warrant shall be the	- Security Service Act Chapter 391 Article 6,7 - Chapter 226 – Terrestrial waters and contiguous zone act Article 6 586.01 (Processing of Personal Data) - Article 4 https://www.fatf-gafi.org/media/fatf/documents/reports/mer-fsrb/Moneyval-Mutual-Evaluation-Report-Malta-2019.pdf

Relevant items	Provisions	Sources used
	interception of or interference with -(a) such communications as are sent to or from one or more addresses specified in the warrant, being an address or addresses likely to be used for the transmission of communications, to or from -(i) one particular person specified or described in the warrant; or(ii) one particular set of premises so specified or described; and(b) such other communications (if any) as it is necessary to intercept or interfere with in order to intercept or interfere with communications falling within paragraph (a).(2) Sub article (1) shall not apply to a warrant if -(a) the interception or interference required by the warrant is the interception or interference, in the course of their transmission by means of a radiocommunications or telecommunication system, of -(i) such external communications as are described in the warrant; and(ii) such other communications (if any) as it is necessary to intercept or interfere with in order to intercept or interfere with such external communications as are so described; and(b) at the time when the warrant is issued, the Minister issues a certificate certifying the descriptions of information the examination of which he considers necessary as mentioned in article 6(3)(a). Surveillance is also mentioned in Chapter 226 – Terrestrial waters and Contiguous zone act under Article 6 6. (1) Any maritime enforcement officer on board a relevant vessel or craft may, within the contiguous zone, take appropriate action with respect to any vessel, other than a foreign military vessel or a ship owned by a foreign state used only for non-commercial service, whether flying the Maltese or any other flag or not flying any flag, reasonably suspected of having on board any person reasonably suspected of being about to commit or of having committed within the jurisdiction of the Maltese courts any relevant offence. (2) Where following appropriate action having been taken in respect of a suspect vessel flying a foreign flag no suspicion remains that an offence against the laws of Malta has been committed by any member of the crew of that vessel, the same vessel may be kept under surveillance until it is out of the limits of the contiguous zone. To add to this, the Processing of Personal Data (SL 586.01) mentions surveillance under Article 4 4. (1) Without prejudice to regulation 10 no person other than the user, shall listen, tap, store or undertake any other form of interception or surveillance of communications and of any related traffic data, without the consent of the user concerned. (2) This regulation shall not affect any legally authorised recording of communications and the related traffic data in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication. Anti-money laundering and counter-terrorist financing measures - Fifth Round Mutual Evaluation Report July 2019 Malta's competent authorities are empowered to use a wide range of investigative techniques for the investigation of ML, associated predicate offences and FT, such as undercover operations (Art. 435E (3) CC), accessing computer systems (Art. 355P and 355Q CC) and controlled deliveries	
Specific range of application of the tool	Data surveillance - computer systems - physical surveillance Whilst the law refers to surveillance as per chapter 391 "interception", in relation to a warrant, includes the possession of, disrupting, destroying, opening, , stopping, seizing, eavesdropping on, surveilling, recording, copying, listening to and viewing of communications and the extraction of information from such communications. The law does not clarify which categories are covered. From the desktop research we have identified that as per the Moneyval evaluation report 2019, the three types of surveillance used in Malta are data surveillance, computer systems and physical surveillance.	https://www.fatf-gafi.org/media/fatf/documents/reports/mer-fsrb/Moneyval-Mutual-Evaluation-Report-Malta-2019.pdf
How is the tool defined?	There is no definition available in the laws of Malta	
For what types of crime can the tool be used?	According to the National intelligence authorities and surveillance in the EU - Malta 2014, Intelligence services can conduct surveillance as long as it is authorised by a warrant issued by the minister in accordance with Articles 6 of the Act. (2) The function of the Service shall be to protect national security and, in particular, against threats from organised crime, espionage, terrorism and sabotage, the activities of agents of foreign powers and against actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means. (3) It shall also be the function of the Service to act in the interests of the economic well-being of Malta; and public safety, in particular, the prevention or detection of serious crime. Financial crimes	https://fra.europa.eu/sites/default/files/fra_uploads/malta-study-data-surveillance-mt.pdf https://www.fatf-gafi.org/media/fatf/documents/reports/mer-fsrb/Moneyval-Mutual-Evaluation-Report-Malta-2019.pdf
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	Judicial authorities grant authorisation to the LEAs to carry out the surveillance needed.	Chapter 391 Security Service Act

Relevant items	Provisions	Sources used
Which LEAs can use this tool?	The Police force, maritime enforcement agencies (Armed forces)	Chapter 391 Security Service Act
What are the rules to be followed for the implementation of this tool?	It has to be authorised by a warrant issued by the Minister, when it comes to the processing of personal data, no other individual can listen to the data other than the authorised user.	- Security Service Act Chapter 391 Article 6,7 - SL 586.01 (Processing of Personal Data) Article 4 - Chapter 391 Social Security Act Article 10
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	10.(1) The requirements of article 6(3)(c) are satisfied in relation to any information if each of the following, namely -(a) the extent to which the information is disclosed;(b) the number of persons to whom any of the information is disclosed;(c) the extent to which the information is copied; and(d) the number of copies made of any of the information, is limited to the minimum that is necessary as mentioned in article6(3)(a).(2) The requirements of 6(3)(a) are satisfied in relation to any intercepted information if each copy made of any of that information is destroyed as soon as its retention is no longer necessary as mentioned in 6(3)(a).	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	A warrant must be issued by the Minister. (3) The Minister may, on an application made by the Security Service, issue or modify a warrant under this article authorising the taking of such action as is specified in the warrant in respect of any property so specified or in respect of any communications so specified if the Minister -(a) thinks it necessary for the action to be taken on the ground that it is likely to be of substantial value in assisting the Service in carrying out any of its functions under this Act; and(b) is satisfied that what the action seeks to achieve cannot reasonably be achieved by other means; and(c) is satisfied that satisfactory arrangements are in force under this Act with respect to the disclosure of information obtained by virtue of this article and that any information obtained under the warrant will be subject to those arrangements.	Security Services Act Chapter 391, Article 6(2) (3)
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Undercover / covert operations		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Code Chapter 9 Article 435E (2) With the same objective of identifying persons involved in the commissions of a criminal offence under the laws of Malta or under the laws of another country, it shall also be lawful for the Attorney General to authorise the Executive Police or a person under the supervision or direction of the Executive Police, to acquire or procure an illicit or suspect consignment of anything from any person or place. (3) Pursuant to any arrangement, including any treaty, convention, agreement or understanding, to which Malta is a party or which is otherwise applicable to Malta, the Attorney General may authorise the competent authorities of another country to conduct in Malta, jointly with or under the supervision or direction of the Executive Police, investigations into criminal offences by officers acting under covert or false identity, provided that the Attorney General is satisfied of the true identity and official capacity of the officers in question and is fully informed of the nature of any documents which purport to guarantee, certify or authenticate the false identity assumed by any such officers. Notwithstanding the provisions of any other law the making or use of such documents by the said competent authorities or by such officers for the purpose or in the course of such investigations authorised as aforesaid shall be deemed to be lawful and shall not entail any liability, civil, criminal or otherwise, on the part of such authorities or officers. (4) Any official from another country taking part in any of the operations referred to in sub articles (1) to (3), both inclusive, shall, for the purpose of any criminal liability incurred under this Code or any other law by that official or by others for conduct against that official, be deemed to be a public officer. (5) The provisions of sub article (4) shall apply mutatis mutandis to any official from another country taking part in any operation in Malta of the kind referred to in sub article (3) even if none of the officers taking part in the operation is acting under covert or false identity Anti-money laundering and counter-terrorist financing measures - Fifth Round Mutual Evaluation Report July 2019 Malta's competent authorities are empowered to use a wide range of investigative techniques for the investigation of ML, associated predicate offences and FT, such as undercover operations (Art. 435E (3) CC), accessing computer systems (Art. 355P and 355Q CC) and controlled deliveries	- Criminal Code Chapter 9 Article 435E https://www.fatf-gafi.org/media/fatf/documents/reports/mer-fsrb/Moneyval-Mutual-Evaluation-Report-Malta-2019.pdf
How is the tool defined?	N/A	

Relevant items	Provisions	Sources used
For what types of crime can the tool be used?	(3) Pursuant to any arrangement, including any treaty, convention, agreement or understanding, to which Malta is a party or which is otherwise applicable to Malta, the Attorney General may authorise the competent authorities of another country to conduct in Malta, jointly with or under the supervision or direction of the Executive Police, investigations into criminal offences by officers acting under covert or false identity, provided that the Attorney General is satisfied of the true identity and official capacity of the officers in question and is fully informed of the nature of any documents which purport to guarantee, certify or authenticate the false identity assumed by any such officers	Criminal Code Chapter 9 Article 435E (1)
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	435E. (1) Notwithstanding anything contained in any other law it shall be lawful for the Attorney General to authorise the Executive Police and, where appropriate, the Customs authorities to allow a controlled delivery to take place with a view to identifying persons involved in the commission of any criminal offence under the laws of Malta or under the laws of another country. The maximum term of imprisonment is not stipulated in the Criminal Code.	Criminal Code Chapter 9 Article 435E
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	The Executive Police and where applicable, customs authorities 435E (1) Notwithstanding anything contained in any other law it shall be lawful for the Attorney General to authorise the Executive Police and, where appropriate, the Customs authorities to allow a controlled delivery to take place with a view to identifying persons involved in the commission of any criminal offence under the laws of Malta or under the laws of another country. There is no reference in the law and no desktop research available in relation to rules which are required when executive police and customs implement this tool	Criminal Code Chapter 9 Article 435E (1)
What are the rules to be followed for the implementation of this tool?	435E (2) With the same objective of identifying persons involved in the commissions of a criminal offence under the laws of Malta or under the laws of another country, it shall also be lawful for the Attorney General to authorise the Executive Police or a person under the supervision or direction of the Executive Police, to acquire or procure an illicit or suspect consignment of anything from any person or place. (4) Any official from another country taking part in any of the operations referred to in sub articles (1) to (3), both inclusive, shall, for the purpose of any criminal liability incurred under this Code or any other law by that official or by others for conduct against that official, be deemed to be a public officer.	Criminal Code Chapter 9 Article 435E (2) (4)
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Authorisation is needed from the Attorney General	Criminal Code Chapter 9 Article 435E (1)
What ongoing supervision is required for the use of this tool?	<u>435E (2)</u> With the same objective of identifying persons involved in the commissions of a criminal offence under the laws of Malta or under the laws of another country, it shall also be lawful for the Attorney General to authorise the Executive Police or a person under the supervision or direction of the Executive Police, to acquire or procure an illicit or suspect consignment of anything from any person or place.	Criminal Code Chapter 9 Article 435E (2)
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	No legislation, however, informants are mentioned in Chapter 9 Criminal Code Article 536/537. The informer shall clearly state the fact with all its circumstances and shall, as far as possible, furnish all such particulars as may be requisite to ascertain the offence, to establish the nature thereof as well as to make known the principals and the accomplices. 537. An information may be laid either verbally or in writing: Provided that where an information is laid verbally, it shall, except in cases which admit of no delay, be reduced to writing forthwith and shall be signed by the informer, or, if he is unable to write, by the Police officer by whom it is reduced to writing.	- Chapter 9 Criminal Code Article 536/537 - Protection of the Whistleblower Act - Chapter 527

Relevant items	Provisions	Sources used
	<u>Protection of the Whistle-blower Act Chapter 527</u> 4. (1) Notwithstanding the provisions of the Criminal Code or of any other law, a whistle-blower who makes a protected disclosure is not liable to any civil or criminal proceedings or to a disciplinary proceeding for having made such a disclosure.(2) The protection afforded to a whistle-blower shall not be prejudiced on the basis only that the whistle-blower making the disclosure was, in good faith, mistaken about its import or that any perceived threat to the public interest on which the disclosure was based has not materialised or that the person making the disclosure has not fully respected the procedural requirements of this Act or of any regulations or guidelines made under this Act.	
Specific range of application of the tool	Anyone can be an informant within the Whistle-blower Act. It is not stipulated in the law that police officers can be covert informants however the Criminal code Chapter 9 Article 435E makes reference to the fact that; it shall also be lawful for the Attorney General to authorise the Executive Police or a person under the supervision or direction of the Executive Police, to acquire or procure an illicit or suspect consignment of anything from any person or place.	• Criminal Code Chapter 9 Article 435E (2)
How is the tool defined?	"whistle-blower" means any employee who makes a disclosure to a whistleblowing reporting officer or a whistleblowing reports unit, as the case may be, whether it qualifies as a protected disclosure or not under this Act;	• Protection of the Whistleblower Act Chapter 527
For what types of crime can the tool be used?	Cross crime areas	• Protection of the Whistleblower Act Chapter 527
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	LEAs use the information given by the informants to be able to investigate further. The law does not clarify whether LEA direct informants during an active investigation.	• Protection of the Whistleblower Act Chapter 527
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	No reference to authorisation is mentioned in either the Protection of the Whistleblower Act or the Criminal Code.	• Protection of the Whistle Blower Act Chapter 527 • Criminal Code Chapter 9 Article 536/537
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	According to the Ministry of Home affairs and security's Annual report of 2013, the drug squad managed to conclude various drug related investigations, with the help of informants.	• https://www.gov.mt/en/Government/Government%20of%20Malta/Ministries%20and%20Entities/Annual%20Government%20Reports/Documents/Annual%20Reports%202013/MHAS.pdf

Source: Author’s own elaboration

The Netherlands

Table 39 – Overview of national rules on investigative tools - Netherlands

Relevant items	Provisions	Sources used
Controlled Delivery		
Relevant documents (legal and non-legal) that define the functioning of the tool	Controlled delivery (<i>in the Dutch CpC this is called: pseudo-purchase or services</i>) by police officers: - article 126i Criminal procedure Code (in case of a crime); and - article 126q Criminal procedure Code (in case of organised crime) - article 126zd, paragraph 1, subsection b, Criminal procedure Code (in case of terrorism) Controlled delivery by civilians: - article 126ij Criminal procedure Code (in case of a crime); and - article 126z Criminal procedure Code (in case of organised crime) - article 126zt, paragraph 1, subsection a, Criminal procedure Code (in case of terrorism)	• Article 126i CpC (in case of a crime) • Article 126q CpC (in case of organised crime) • Article 126ij CpC (in case of a crime) • Article 126z CpC (in case of organised crime) • Article 126zd CpC (in case of terrorism) • Article 126zt CpC (in case of terrorism)

Relevant items	Provisions	Sources used
How is the tool defined?	Please refer to Article 126i Criminal procedure Code: 1. In case of a suspicion of an offence as defined in article 67, first paragraph, the public prosecutor has the competence, in the interest of the investigation, to order that an investigating officer: - purchases goods from the suspect; - data that is stored, processed or transferred by means of an automated work, through a public telecommunications network, obtains from the suspect, - provides services to the suspect. 2. the investigating officer, during the execution of the warrant, is prohibited from inducing a suspect to commit other criminal offenses than those on which his intent was previously aimed. 3. The warrant to pseudo-purchase or services is in writing and contains/mentions the following: a. the offence, and if known, the name or otherwise a description of the suspect that is as accurate as possible; b. the facts or circumstances from which it appears that the conditions referred to in the first paragraph have been fulfilled; c. the nature of the goods, data or services; d. the manner in which the warrant is executed, including criminalised behaviour; e. the time when or the period within which the warrant will be executed.	Article 126i Criminal procedure Code
For what types of crime can the tool be used?	Please refer to article 67, first paragraph, Criminal procedure Code: this tool can be used by both police officers and <i>civilians can provide assistance to the investigation by applying this investigative tool</i> for the following types of crimes: a) every crime which, according to the legal definition, is punishable by imprisonment of four years or more, whether or not committed in an organised context; b) specific crimes mentioned in the Criminal procedure Code; c) specific crimes mentioned in other bills, such as: the Gas Act, the Animals Act, Road Traffic Act, Opium Act etc. (not exhaustive). The above conditions cover all the SOC's mentioned, so the tool applies to all types of serious and organised crime, including terrorism.	Article 67 Criminal procedure Code
Does national law allow this tool to be used in cross border cases?	No	
What thresholds must be passed for the use of this tool?	An imprisonment of four years or more. In the Netherlands imprisonment can be temporary (up to a maximum of 30 years) or life imprisonment.	
What types of stakeholder are involved in the implementation of this tool?	When pseud- purchase or services is used by police officers, please refer to article 126i Criminal procedure Code: 1. there must be a reasonable suspicion of a crime as defined in article 67, first paragraph, Criminal procedure Code; 2. the tool can only be applied in the interest of the investigation; 3. when pseudo-purchase or services is applied, it may not induce the suspect to commit other criminal offenses than those on which his intent was previously aimed; 4. the warrant to pseudo-purchase or services must be in writing and must state the following: a. the offence, and if known, the name or otherwise a description of the suspect that is as accurate as possible; b. the facts or circumstances from which it appears that the conditions referred to in the first paragraph have been fulfilled; c. the nature of the goods, data or services; d. the manner in which the warrant is executed, including criminalised behaviour; e. the time when or the period within which the warrant will be executed. 5. if applicable, the conditions as defined in article 126g, paragraph six to eight, CpC also apply. As a consequence: a) In urgent need, the warrant may be given orally. In that case, the public prosecutor will put the order in writing within three days. b) As soon as the conditions referred to in the first and bullets are no longer met, the public prosecutor will determine that the execution of the warrant is terminated. c) The warrant may be amended, supplemented, extended or terminated in writing and with reasons. In case of urgent need, the decision can be made orally. In that case, the public prosecutor will put this in writing within three days. Please note that in case of organised crimes, similar conditions must be met. Please refer to article 126q Criminal procedure Code for more detail. When the tool is applied by civilians, similar conditions must be met. But the tool can only be used by civilians if the tool cannot be used by investigating officers. Please refer to article 126ij Criminal procedure Code, and in case of organised crime, please refer to article 126z Criminal procedure Code.	
Which LEAs can use this tool?	1. the public prosecutor who can issue the warrant;	

Relevant items	Provisions	Sources used
	2. the investigating officer who can apply the tool; 3. a civilian, who can apply the tool if application by an investigating officer is not possible.	
What are the rules to be followed for the implementation of this tool?	1. Public Prosecutor 2. Investigating officer (police officer)	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Please refer to the conditions as described in D10 above.	
What authorisation is needed for the use of this tool?	A warrant. This warrant must be in writing and must state the following: - the offence, and if known, the name or otherwise a description of the suspect that is as accurate as possible; - the facts or circumstances from which it appears that the conditions referred to in the first paragraph have been fulfilled; - the nature of the goods, data or services; - the manner in which the warrant is executed, including criminalized behaviour (only applicable if the tool is applied by a investigating officer); - the time when or the period within which the warrant will be executed. (only applicable if the tool is applied by a investigating officer); Please refer to article 126i, third paragraph Criminal procedure Code and article 126q, third paragraph, Criminal procedure Code. Please note that in the case of application of the tool by a civilian, in addition to a warrant, an agreement to pseudo-purchase or services is needed. This agreement must be in writing and must contain the following: - the rights and obligations of the person (civilian) who provides assistance with the investigation, as well as the manner in which the agreement is applied, including criminal behaviour, and - the time at which or the period within which the agreement is performed. Please refer to article 126ij CpC jo. 126w, paragraph seven and eight, Criminal procedure Code	
What ongoing supervision is required for the use of this tool?	- In urgent need, the warrant may be given orally. In that case, the public prosecutor will put the order in writing within three days. - As soon as the conditions are no longer met, the public prosecutor will determine that the execution of the warrant is terminated. - The warrant may be amended, supplemented, extended or terminated in writing and with reasons. In case of urgent need, the decision can be made orally. In that case, the public prosecutor will put this in writing within three days. Please refer to articles 126i Criminal procedure Code jo. 126g, paragraph six to eight, Criminal procedure Code In case of application of the tool by civilians: - the person (civilian) who provides assistance with the investigation, is prohibited from committing criminal offences during the execution thereof, unless prior written permission has been given by the public prosecutor to commit such offences. - As soon as the conditions are no longer met, the public prosecutor will determine that the execution of the warrant is terminated. Please refer to article 126ij Criminal procedure Code jo. article 126w, seventh and eight paragraph, Criminal procedure Code	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Data available on the number of times this tool has been used for SOC cases	N/A	
Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	Hot pursuit within the Netherlands: Article 53, 54, 55 and 55a Criminal procedure Code Hot pursuit cross-border: Article 41 Schengen Agreement	- Article 53 CpC - Article 54 CpC - Article 12 Enschede Treaty - Article 21 Benelux Treaty
How is the tool defined?	Hot pursuit in the act of committing an offence (please refer to article 53 Criminal procedure Code): 1. If a criminal offense is discovered in the act, everyone is authorised to arrest the suspect.	

Relevant items	Provisions	Sources used
	2. The investigating officer who arrests a suspect in the act when discovered, shall transport him or her as soon as possible to the place for questioning to be presented to the assistant public prosecutor or the public prosecutor. 3. If the arrest is carried out by someone other than an investigating officer, that person will immediately hand over the person arrested to an investigating officer, including objects found at the suspect. The investigating officer acts in accordance with the provision of the second paragraph and draws up a seizure notice if necessary. 4. When the suspect is brought before the assistant public prosecutor or the public prosecutor, the latter assesses the need for further deprivation of liberty on the basis of Article 56a. Hot pursuit not in the act of committing an offence (please refer to article 54, Criminal procedure Code): 1. Apart from the case of discovery in the act, the investigating officer is authorised, by order of the public prosecutor, to arrest the suspect of a crime for which pre-trial detention has been admitted in order to bring him or her before the assistant public prosecutor or the public prosecutor as soon as possible. 2. The warrant of arrest can be given orally or in writing by the public prosecutor. If given orally, it should be stated afterwards in the official report. 3. If the order of the public prosecutor cannot be awaited, the authority referred to in the first paragraph shall accrue to the assistant public prosecutor. The assistant public prosecutor shall immediately notify the public prosecutor in writing or orally of the arrest. The second paragraph applies mutatis mutandis. 4. If the order of the public prosecutor or the assistant public prosecutor cannot be awaited, the investigating officer is authorised to arrest the suspect in order to bring him or her before the assistant public prosecutor or the public prosecutor as soon as possible. 5. The power to arrest, other than the case of discovery in the act, belongs to a person in the public service of a foreign state who exercises the right of pursuit in the Netherlands across-borders in a manner permitted by international law, under the obligation to act with regard to the person arrested in accordance with Article 53, second paragraph. Hot pursuit cross-border (Please refer to article 41 Schengen Agreement): 1. Officers of one of the Contracting Parties who are pursuing in their country an individual caught in the act of committing or of participating in one of the offences referred to in paragraph 4 shall be authorised to continue pursuit in the territory of another Contracting Party without the latter's prior authorisation where, given the particular urgency of the situation, it is not possible to notify the competent authorities of the other Contracting Party by one of the means provided for in Article 44 prior to entry into that territory or where these authorities are unable to reach the scene in time to take over the pursuit. The pursuing officers shall, not later than when they cross the border, contact the competent authorities of the Contracting Party in whose territory the hot pursuit is to take place. The hot pursuit will cease as soon as the Contracting Party in whose territory the pursuit is taking place so requests. At the request of the pursuing officers, the competent local authorities shall challenge the pursued person in order to establish the person's identity or to make an arrest.	
For what types of crime can the tool be used?	Hot pursuit within the Netherlands: a. in the act: the tool can be used to every criminal offence, including terrorism b. not in the act: the tool can be used for criminal offences for which remand to custody is permitted (i.e., every criminal offence which, according to the legal definition, is punishable by imprisonment of four years or more, this covers terrorism). Hot pursuit cross-border Murder, manslaughter, rape, arson, forgery of money, aggravated burglary and robbery and receiving stolen goods, extortion, kidnapping and hostage taking, trafficking in human beings, illicit trafficking in narcotic drugs and psychotropic substances, breach of the laws on arms and explosives, wilful damage through the use of explosives, illicit transportation of toxic and hazardous waste, failure to stop and give particulars after an accident which has resulted in death or serious injury. Please refer to article 41, paragraph 4, Schengen Agreement.	
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	An imprisonment of one day or more. In the Netherlands imprisonment can be temporary (up to a maximum of 30 years) or life imprisonment.	
What types of stakeholder are involved in the implementation of this tool?	1. Everyone (in case of hot pursuit in the act within the Netherlands) 2. Investigating officer (police officer), in case of hot pursuit not in the act within the Netherlands or in case of cross-border hot pursuit 3. Public prosecutor to issue warrant to hot pursuit	

Relevant items	Provisions	Sources used
Which LEAs can use this tool?	- Everyone (in case of hot pursuit in the act within the Netherlands) - Investigating officer (police officer), in case of hot pursuit not in the act within the Netherlands or in case of cross-border hot pursuit - Public prosecutor to issue the warrant to hot pursuit	
What are the rules to be followed for the implementation of this tool?	Please refer to D23: Investigating officers (police officers) and the Public Prosecutor	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	In case of hot pursuit in the act: no authorisation is needed. In case of hot pursuit not in the act of committing an offence within the Netherlands and cross-border: a warrant from the public prosecutor.	
Is there any national case law relating to the use of this tool in cross-border crime cases?	Please refer to the conditions as described in D20 above.	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	Witness protection is covered by: - Article 226l Criminal procedure Code Witness+C36:D37s protection is possible with regard to the following types of witnesses: - threatened witnesses (please refer to article 226a Criminal procedure Code) - witnesses who are also suspects (please refer to article 226g Criminal procedure Code, in combination with art. 44a Sr, since it deals with reduced sentences.) - witnesses who have already been convicted (please refer to article 226k Criminal procedure Code) - shielded witnesses (please refer to article 226m Criminal procedure Code, in case of state security)	• <i>Article 226l CpC</i> • <i>Article 226a CpC</i> • <i>Article 226g CpC</i> • <i>Article 226k CpC</i> • <i>Article 226m</i>
How is the tool defined?	Please refer to article 22l Criminal procedure Code: - Our Minister of Security and Justice may, in a manner to be determined by order in council, take specific measures for the actual protection of witnesses, as referred to in Articles 226a, 226g, 226k and 226m. - Subsection 1 shall apply mutatis mutandis to a person who has cooperated with the authorities charged with the investigation and prosecution of criminal offenses, insofar as an urgent need has arisen as a result of such cooperation and related government action. - Our Minister of Security and Justice may appoint officials charged with the investigation of criminal offenses. In implementation of the provisions of the first and second paragraph, these officials are authorised to turn to anyone for cooperation in the factual protection to be provided. If the cooperation referred to in the third paragraph is not provided, the public prosecutor may demand this cooperation in the interest of the actual protection of the witness. - The applicable statutory regulations with regard to the cooperation referred to in the third and fourth paragraph remain inapplicable, insofar as they prevent the cooperation. - The person to whom a request for cooperation as referred to in the third paragraph or a claim as referred to in the fourth paragraph is addressed, will observe secrecy in the interest of the factual protection of the witness about all that is known to him regarding the request for cooperation or the claim. - A claim as referred to in the fourth paragraph cannot be addressed to the suspect. Section 96a, subsection 3 shall apply mutatis mutandis.	
For what types of crime can the tool be used?	Witness protection is possible <u>for every crime</u> regarding the following witnesses: - threatened witnesses (please refer to article 226a Criminal procedure Code) - witnesses who have already been convicted (please refer to article 226k Criminal procedure Code) - shielded witnesses (please refer to article 226m Criminal procedure Code) regarding witnesses who are also suspects: A deal with witness as referred to in art.226g can only apply on testimonies on crimes described in art. 67, 1, SV. Crimes must have taken place	

Relevant items	Provisions	Sources used
	in an organized capacity, must have shocked the rule of law and be sentenced with at least 8 years. Idem for 226 witnesses	
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	An imprisonment of one day or more. In the Netherlands imprisonment can be temporary (up to a maximum of 30 years) or life imprisonment.	
What types of stakeholder are involved in the implementation of this tool?	1. Magistrate who grants the authorisation at the request of the public prosecutor; 2. The public prosecutor who can issue the warrant to provide data; 3. The investigating officer who can apply the tool.	
Which LEAs can use this tool?	1. Public Prosecutor; 2. Investigating officer (police officer)	
What are the rules to be followed for the implementation of this tool?	<u>In case of a threatened witness (please refer to article 226a Criminal procedure Code):</u> The examining magistrate may order, either ex officio or at the request of the public prosecutor or of the suspect or the witness, that his identity be concealed during the interrogation of that witness, if: a. the witness or another person may, by virtue of the statement to be made by the witness, consider himself / herself threatened to such an extent that it must be reasonably assumed that the life, health or safety or the disruption of the family life or the socio-economic existence of that witness or other person is to be feared, and b. the witness has indicated that he does not wish to make a statement because of this threat. <u>in case of a witnesses who are also suspects (please refer to article 226g Criminal procedure Code) + in case of a witnesses who have already been convicted (please refer to article 226k Criminal procedure Code)</u> an agreement that has been put in writing and contains as accurate a description as possible of: - the crimes about which and, if possible, the suspect against whom the witness referred to in the first paragraph is prepared to give a testimony; - the offenses for which the witness in the case in which he is himself a suspect will be prosecuted and to which this undertaking relates; - the conditions imposed on the witness, who is also the suspect, and which he is prepared to comply with; - the content of the commitment of the public prosecutor. <u>in case of a shielded witness (please refer to article 226m Criminal procedure Code)</u> The examining magistrate orders, either ex officio or at the request of the public prosecutor or at the request of the suspect or the witness, that a witness be heard as a protected witness if, in all reasonableness, the interest of state security must be that demands. Rules for general protective measures: "If an order to take protective measures has been issued, the public prosecutor concludes a written agreement with the person to be protected, which in any case includes provisions regarding the obligations of the person to be protected and the witness protection component as well as the consequences of non-compliance thereof." (See art. 7 Witness Protection Decree)	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Please refer to the conditions as described in D43 above.	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	1. An order of the Magistrate (in case of threatened witnesses or shielded witnesses), please refer to article 226a and 226m Criminal procedure Code; 2. a written agreement assessed by the magistrate (in case of witnesses who are also suspects or witnesses who have already been convicted), please refer to article 226g, third paragraph, and 226k Criminal procedure Code)	
What ongoing supervision is required for the use of this tool?	Please refer to the conditions as described above.	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Surveillance		

Relevant items	Provisions	Sources used
Relevant documents (legal and non-legal) that define the functioning of the tool	Surveillance (i.e. systematic observation) by an investigating officer: - Article 126g Criminal procedure Code (in case of a crime); and - Article 126o Criminal procedure Code (in case of organised crime) - article 126zd Criminal procedure Code, paragraph 1, subsection a, Criminal procedure Code (in case of terrorism) Recording confidential information by an investigating officer: - Article 126l Criminal procedure Code (in case of a crime) - Article 126s Criminal procedure Code (in case of organised crime) Recording telecommunication by an investigating officer: - Article 126m Criminal procedure Code (in case of a crime) - Article 126t Criminal procedure Code (in case of an organised crime) Claim data / information - Article 126nc up to and including 126ni Criminal procedure Code	• Article 126g CpC (in case of a crime) • Article 126o CpC (in case of organised crime) • Article 126zd CpC (in case of terrorism) • Article 126l CpC (in case of a crime) • Article 126s CpC (in case of organised crime) • Article 126m CpC (in case of a crime) • Article 126t CpC (in case of an organised crime) • Article 126nc up to and including 126ni CpC
Specific range of application of the tool	Please refer to D42 above. These articles cover: audio surveillance, visual surveillance, tracking surveillance and data surveillance.	
How is the tool defined?	Please refer to article 126g, Criminal procedure Code: 1. In the event of a suspicion of a crime, the public prosecutor may, in the interest of the investigation, order an investigating officer to systematically monitor a person or systematically observe their presence or behaviour. 2. If the suspicion concerns a crime as described in Article 67, first paragraph, which constitutes a serious violation of the legal order, in view of its nature or the connection with other crimes committed by the accused, the public prosecutor may determine in the interest of the investigation that for the execution of the warrant, a private place, not being a house, is entered without the consent of the entitled party. 3. The public prosecutor may determine that a technical aid is used to execute the warrant, insofar as no confidential communication is recorded. A technical aid is not attached to a person, unless with his permission or in the case referred to in Article 126nba, first paragraph, under c. 4. The warrant is issued for a maximum period of three months. It can be extended each time for a maximum period of three months. 5. This warrant to surveillance must be in writing and must state the following: a. the crime and if known the name or otherwise an as accurate as possible description of the suspect; b. the facts or circumstances from which it appears that the conditions, referred to in the first paragraph, have been fulfilled; c. the name or as accurate as possible an indication of the person referred to in the first paragraph; d. in application of the second paragraph, the facts or circumstances from which it appears that the conditions referred to in that paragraph have been fulfilled, as well as the place that will be entered; e. the manner in which the order will be executed, and f. the period of validity of the order. 6. In urgent need, the order may be given orally. In that case, the public prosecutor will put the order in writing within three days. 7. As soon as the conditions referred to in the first paragraph are no longer met, the public prosecutor will determine that the execution of the order is terminated. 8. The order may be amended, supplemented, extended or terminated in writing and with reasons. In case of urgent need, the decision can be made orally. In that case, the public prosecutor will put this in writing within three days. 9. An order as referred to in paragraph 1 may also be given to a person in the public service of a foreign state. Requirements may be imposed on these persons by order in council. Subsections 2 to 8 apply mutatis mutandis.	
For what types of crime can the tool be used?	Please refer to article 126g Criminal procedure Code and article 126o Criminal procedure Code: this tool can be applied by both police officers and civilians in case of: - a suspicion of a crime; - a reasonable suspicion that crime as described in Article 67, first paragraph, CpC is planned or committed in organised context. The above conditions cover all the SOC's mentioned, so the tool applies to all types of serious and organised crime. Please note that similar conditions apply with regard to the recording of confidential information (please refer to article 126l and article 126s CpC) and to the recording of telecommunication (please refer to article 126t CpC).	
Does national law allow this tool to be used in cross border cases?	Please refer to article 126g, fourth to seventh paragraph, Criminal procedure Code: 1. there must be a reasonable suspicion of a crime; 2. the tool can only be applied in the interest of the investigation;	

Relevant items	Provisions	Sources used
	3. The warrant is issued for a maximum period of three months. It can be extended each time for a maximum period of three months. 4. the warrant to surveillance must be in writing and must state the following: - the offence, and if known, the name or otherwise a description of the suspect that is as accurate as possible; - the facts or circumstances from which it appears that the conditions referred to in the first paragraph have been fulfilled; - the name or as accurate as possible an indication of the person referred to in the first paragraph; - in application of the second paragraph, the facts or circumstances from which it appears that the conditions referred to in that paragraph have been fulfilled, as well as the place that will be entered; - the manner in which the order will be executed, and - the period of validity of the order. 6. In urgent need, the warrant may be given orally. In that case, the public prosecutor will put the order in writing within three days. 7. As soon as the conditions referred to in the first bullet are no longer met, the public prosecutor will determine that the execution of the warrant is terminated. 8. The warrant may be amended, supplemented, extended or terminated in writing and with reasons. In case of urgent need, the decision can be made orally. In that case, the public prosecutor will put this in writing within three days. Please note that in case of organised crimes, similar conditions must be met. Please refer to article 126o CpC for more detail.	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	An imprisonment of one day or more. In the Netherlands imprisonment can be temporary (up to a maximum of 30 years) or life imprisonment.	
Which LEAs can use this tool?	- The public prosecutor who can issue the warrant; - The investigating officer who can apply the tool.	
What are the rules to be followed for the implementation of this tool?	- Public Prosecutor - Investigating officer (police officer)	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Please refer to the conditions as described in D46 above.	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Please refer to the conditions as described in D46 above.	
What ongoing supervision is required for the use of this tool?	A warrant. This warrant to surveillance must be in writing and must state the following: - the offence, and if known, the name or otherwise a description of the suspect that is as accurate as possible; - the facts or circumstances from which it appears that the conditions referred to in the first paragraph have been fulfilled; - the name or as accurate as possible an indication of the person referred to in the first paragraph; - in application of the second paragraph, the facts or circumstances from which it appears that the conditions referred to in that paragraph have been fulfilled, as well as the place that will be entered; - the manner in which the order will be executed, and - the period of validity of the order. Please note that similar conditions apply with regard to the recording of confidential information (please refer to article 126l and article 126s Criminal procedure Code) and to the recording of telecommunication (please refer to article 126t Criminal procedure Code).	
Is there any national case law relating to the use of this tool in cross-border crime cases?	Please refer to article 126g, paragraph six to eight, CpC: - In urgent need, the warrant may be given orally. In that case, the public prosecutor will put the order in writing within three days. - As soon as the conditions are no longer met, the public prosecutor will determine that the execution of the warrant is terminated. - The warrant may be amended, supplemented, extended or terminated in writing and with reasons. In case of urgent need, the decision can be made orally. In that case, the public prosecutor will put this in writing within three days. Please note that similar conditions apply with regard to the recording of confidential information (please refer to article 126l and article 126s Criminal procedure Code) and to the recording of telecommunication (please refer to article 126t Criminal procedure Code).	

Relevant items	Provisions	Sources used
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N.A.	
Undercover / covert operations		
Relevant documents (legal and non-legal) that define the functioning of the tool	Systematic collection of information by investigating officer: - Article 126j Criminal procedure Code (in case of a crime); and - Article 126qa Criminal procedure Code (in case of organised crime) - article 126zd Criminal procedure Code, paragraph 1, subsection c, Criminal procedure Code (in case of terrorism) Systematic gathering of information by civilians: - Article 126v Criminal procedure Code - article 126zt Criminal procedure Code, paragraph 1, subsection b, Criminal procedure Code (in case of terrorism)	• Article 126j CpC (in case of a crime) • Article 126qa CpC (in case of organised crime) • Article 126zd CpC • Article 126v CpC • Article 126zt CpC
How is the tool defined?	Please refer to article 126j, paragraph one to three, Criminal procedure Code: 1. In the event of a suspicion of a crime, the public prosecutor may, in the interest of the investigation, order that an investigating officer as referred to in Articles 141, parts, b, c and d, and 142, without it being known that he is acting as an investigating officer, systematically collect information about the suspect. 2. The order is issued for a maximum period of three months. The period of validity can be extended each time for a maximum period of three months. 3. The warrant to inquiry of information is in writing and must state the following: a. the crime and if known the name or otherwise a description of the suspect that is as accurate as possible; b. the facts or circumstances from which it appears that the conditions referred to in the first paragraph have been fulfilled; c. the manner in which the order is executed, and d. the period of validity of the order. 6. Section 126g, subsections 7 and 8, shall apply mutatis mutandis.	
For what types of crime can the tool be used?	Please refer to article 126j Criminal procedure Code and article 126qa Criminal procedure Code: this tool can be applied by both police officers and civilians in case of: - a suspicion of a crime, including terrorism; - a reasonable suspicion that crime as described in Article 67, first paragraph, Criminal procedure Code is planned or committed in organised context. The above conditions cover all the SOC's mentioned, so the tool applies to all types of serious and organised crime.	
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	An imprisonment of one day or more. In the Netherlands imprisonment can be temporary (up to a maximum of 30 years) or life imprisonment.	
What types of stakeholder are involved in the implementation of this tool?	When the tool is used by police officers, please refer to article 126j, Criminal procedure Code: 1. there must be a reasonable suspicion of a crime; 2. The warrant is issued for a maximum period of three months. The period of validity can be extended each time for a maximum period of three months. 3. the warrant to must be in writing and must state the following: a. the crime and if known the name or otherwise a description of the suspect that is as accurate as possible; b. the facts or circumstances from which it appears that the conditions referred to in the first paragraph have been fulfilled; c. the manner in which the order is executed, and d. the period of validity of the order. 4. if applicable, the conditions as defined in article 126g, paragraph six to eight, CpC also apply. As a consequence: a) In urgent need, the warrant may be given orally. In that case, the public prosecutor will put the order in writing within three days. b) As soon as the conditions referred to in the first bullet are no longer met, the public prosecutor will determine that the execution of the warrant is terminated. c) The warrant may be amended, supplemented, extended or terminated in writing and with reasons. In case of urgent need, the decision can be made orally. In that case, the public prosecutor will put this in writing within three days. Please note that in case of organised crimes, similar conditions must be met. Please refer to article 126qa, Criminal procedure Code for more detail.	

Relevant items	Provisions	Sources used
	When the tool is applied by <i>as explained above</i> , this tool can be applied by civilians to provide assistance to the investigation], similar conditions must be met. Please refer to article 126v, CpC.	
Which LEAs can use this tool?	1. The public prosecutor who can issue the warrant; 2. The investigating officer who can apply the tool; 3. A civilian, who can apply the tool if there is a reasonable suspicion that crime as described in Article 67, first paragraph, Criminal procedure Code is planned or committed in organised context.	
What are the rules to be followed for the implementation of this tool?	1. Public Prosecutor; 2. Investigating officer (police officer)	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Please refer to the conditions as described above.	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Please refer to the conditions as described above.	
What ongoing supervision is required for the use of this tool?	A warrant. This warrant must be in writing and must state the following: a. the warrant to information collection must be in writing and must state the following: a. the offence, and if known, the name or otherwise a description of the suspect that is as accurate as possible; b. the facts or circumstances from which it appears that the conditions referred to in the first paragraph have been fulfilled; c. the manner in which the warrant is executed, including criminalised behaviour; d. the period of validity of the warrant. Please refer to article 126j, third paragraph, Criminal procedure Code. In case of crimes as described in Article 67, first paragraph, Criminal procedure Code which are planned or committed in organised context, similar conditions apply. Please refer to article 126qa, third paragraph, Criminal procedure Code. Please note that in the case of application of the tool by a civilian, in addition to a warrant, an agreement to systematically obtain information is needed. This agreement must be in writing and must contain the following: a. the rights and obligations of the person (civilian) who provides assistance with the investigation, as well as the manner in which the agreement is applied, and b. the time at which or the period within which the agreement is performed. Please refer to article 126v, paragraph three, Criminal procedure Code.	
Is there any national case law relating to the use of this tool in cross-border crime cases?	a. In urgent need, the warrant may be given orally. In that case, the public prosecutor will put the order in writing within three days. b. As soon as the conditions are no longer met, the public prosecutor will determine that the execution of the warrant is terminated. c. The warrant may be amended, supplemented, extended or terminated in writing and with reasons. In case of urgent need, the decision can be made orally. In that case, the public prosecutor will put this in writing within three days. Please refer to articles 126j Criminal procedure Code jo. 126g, paragraph six to eight, Criminal procedure Code In case of application of the tool by civilians the same conditions apply. Please refer to article 126v Criminal procedure Code jo. article 126g, fourth, sixth till eight paragraph, Criminal procedure Code	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	Use of informants/infiltration: police officers: - article 126h Criminal procedure Code (in case of a crime); and - article 126p Criminal procedure Code (in case of organised crime) - article 126ze Criminal procedure Code (in case of terrorism) Use of informants/infiltration: civilians: - article 126w Criminal procedure Code (in case of a crime); and - article 126x Criminal procedure Code (in case of organised crime) - article 126zu Criminal procedure Code (in case of terrorism)	- Article 126h CpC (in case of a crime) - Article 126p CpC (in case of organised crime) - Article 126ze CpC - Article 126w CpC (in case of a crime) - Article 126x CpC (in case of organised crime) - Article 126zu CpC
Specific range of application of the tool	To apply this tool, it is required that cooperation is given to a group of persons in which very serious crimes are planned or committed. There are no specific requirements for the group, this can also be a network or a legal organisation within which a group of people plan or commit very	

Relevant items	Provisions	Sources used
	serious crimes. This tool (i.e. infiltration) can be applied by investigating officers (police officers) and civilians (i.e. members of the public).	
How is the tool defined?	Please refer to article 126h Criminal procedure Code: 1. In the event of a criminal offense as described in Article 67, paragraph 1, which constitutes a serious breach of the legal order, in view of its nature or the connection with other offenses committed by the accused, the public prosecutor may, if the investigation so requires, order that an investigating officer as referred to in articles 141, parts, b, c and d, and 142, participates or cooperates with a group of persons in which it can reasonably be suspected that crimes are being planned or committed. 2. The investigating officer, during the execution of the warrant, is prohibited from inducing a suspect to commit other criminal offences other than those on which his intent was previously aimed. 3. The warrant for infiltration is in writing and states: a. the crime and if known the name or otherwise a description of the suspect that is as accurate as possible; b. a description of the group of persons; c. the facts or circumstances from which it appears that the conditions referred to in the first paragraph have been fulfilled; d. the manner in which the warrant will be executed, including acts made punishable, insofar as foreseeable when giving the warrant, and e. the period of validity of the warrant. 6. Section 126g, subsections 7 and 8, shall apply mutatis mutandis, on the understanding that extension of an order for infiltration cannot take place verbally.	
For what types of crime can the tool be used?	Please refer to article 67, first paragraph, Criminal procedure Code: this tool can be used by both police officers and civilians for the following types of crimes: a) every crime which, according to the legal definition, is punishable by imprisonment of four years or more, whether or not committed in an organised context , including terrorism; b) specific crimes mentioned in the Criminal procedure Code; c) specific crimes mentioned in other bills, such as: the Gas Act, the Animals Act, Road Traffic Act, Opium Act etc. (not exhaustive). The above conditions cover all the SOC's mentioned, so the tool applies to all types of serious and organised crime.	
Does national law allow this tool to be used in cross border cases?	No	
What thresholds must be passed for the use of this tool?	An imprisonment of four years or more. In the Netherlands imprisonment can be temporary (up to a maximum of 30 years) or life imprisonment.	
What types of stakeholder are involved in the implementation of this tool?	When the tool is used by police officers, please refer to article 126h Criminal procedure Code: 1. there must be a suspicion of a crime as defined in article 67, first paragraph, Criminal procedure Code; 2. this crime as referred to under 1, must constitute a serious breach of the legal order; 3. the tool can only be applied if the investigation requires this urgently; 4. when the tool is applied, it may not induce the suspect to commit other criminal offenses than those on which his intent was previously aimed; 4. the warrant to infiltration must be in writing and must state the following: a. the offence, and if known, the name or otherwise a description of the suspect that is as accurate as possible; b. the facts or circumstances from which it appears that the conditions referred to in the first paragraph have been fulfilled; c. the nature of the goods, data or services; d. the manner in which the warrant is executed, including criminalised behaviour; e. the time when or the period within which the warrant will be executed; 5. if applicable, the conditions as defined in article 126g, paragraph six to eight, Criminal procedure Code also apply. As a consequence: a) As soon as the conditions referred to in the first bullet are no longer met, the public prosecutor will determine that the execution of the warrant is terminated. b) The warrant may be amended, supplemented, extended or terminated in writing and with reasons. Please note that in case of organised crimes, similar conditions must be met. Please refer to article 126p Criminal procedure Code for more detail. When the tool is applied by civilians, similar conditions must be met. But the tool can only be used by civilians if the tool cannot be used by investigating officers. Please refer to article 126w Criminal procedure Code, and in case of organised crime, please refer to article 126x Criminal procedure Code.	
Which LEAs can use this tool?	1. The public prosecutor who can issue the warrant to infiltration/use of informants;	

Relevant items	Provisions	Sources used
	2. The investigating officer who can apply the tool; 3. A civilian, who can apply the tool if application by an investigating officer is not possible.	
What are the rules to be followed for the implementation of this tool?	1. Public Prosecutor 2. Investigating officer (police officer)	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Please refer to the conditions as described above.	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Please refer to the conditions as described above.	
What ongoing supervision is required for the use of this tool?	A warrant. This warrant must be in writing and must state the following: a. the crime and if known the name or otherwise a description of the suspect that is as accurate as possible; b. a description of the group of persons; c. the facts or circumstances from which it appears that the conditions referred to in the first paragraph have been fulfilled; d. the manner in which the warrant will be executed, including acts made punishable, insofar as foreseeable when giving the warrant, and e. the period of validity of the warrant. Please refer to article 126h, third paragraph Criminal procedure Code and article 126q, third paragraph, Criminal procedure Code. Please note that in the case of application of the tool by a civilian, in addition to a warrant, an agreement to infiltration/informants is needed. This agreement must be in writing and must contain the following: a. the rights and obligations of the person (civilian) who provides assistance with the investigation, as well as the manner in which the agreement is applied, including criminal behaviour, and b. the time at which or the period within which the agreement is performed. Please refer to article 126w and 126x Criminal procedure Code	
Is there any national case law relating to the use of this tool in cross-border crime cases?	a. the warrant to apply the tool must be in writing and cannot be given orally. b. As soon as the conditions are no longer met, the public prosecutor will determine that the execution of the warrant is terminated. c. The warrant may be amended, supplemented, extended or terminated in writing and with reasons. Please refer to articles 126h Criminal procedure Code jo. 126g, paragraph seven and eight, Criminal procedure Code In case of application of the tool by civilians: a) the person (civilian) who provides assistance with the investigation, is prohibited from committing criminal offences during the execution thereof, unless prior written permission has been given by the public prosecutor to commit such offences. b) As soon as the conditions are no longer met, the public prosecutor will determine that the execution of the warrant is terminated. c) the agreement may be amended, supplemented, extended or terminated in writing and with reasons. Please refer to articles 126w and 126x Criminal procedure Code.	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	

Source: Author's own elaboration

Norway

Table 40 – Overview of national rules on investigative tools - Norway

Relevant items	Provisions	Sources used
Controlled Delivery		
Relevant documents (legal and non-legal) that define the functioning of the tool	The National Law does NOT defines this tool. It follows the UN treaty to fight against organised crime in cross-border cases. This treaty signed by Norway in 13/12/2000.	
How is the tool defined?	N/A	

Relevant items	Provisions	Sources used
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Data available on the number of times this tool has been used for SOC cases	N/A	
• Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	N/A	
How is the tool defined?	N/A	
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Procedure Act	• DETKONGELIGEJUSTIS-OG BEREDSKAPSDEPARTMENT, Ministry of Justice and Public Security, Act of 22 May 1981 No. 25. With subsequent amendments, the latest made by • Act of 21 June 2013 No. 84

Relevant items	Provisions	Sources used
How is the tool defined?	This tool is NOT properly defined in the national law. Whereas, it gives the general or broad information- "Unless otherwise provided by statute, every person summoned to attend as a witness is bound to do so and to give evidence before the court."	Section 108
For what types of crime can the tool be used?	Witness protection can be given when violation of sections Terrorist acts (section 132 a), trafficking of fire arms (section 189, 190, 191), conspiracy to commit serious crimes (section 198), human trafficking (section 256) of the Penal Code	- Section 130 a of witness protection act. - Section 132, 189, 190, 191, 198 and 256 of Penal Code. Link https://lovdata.no/dokument/NLE/lov/2005-05-20-28/*&#x2a;
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	LEAs	Section 109
Which LEAs can use this tool?	LEAs	- Section 109 - Section 110, para 1
What are the rules to be followed for the implementation of this tool?	A witness shall be summoned by service of a witness summons. The summons shall specify the case and the purpose of the summons, the court, the place of sitting, and the time of attendance. It shall also contain brief information about the rules relating to allowances for witnesses and about the liability for failure to attend. As far as possible the witness should be given at least three days' notice.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Investigating judge can grant the permission upon the request of Public Prosecutor. Investigating judge upon request of the public prosecutor	- Section 130 a. - Section 109
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Surveillance		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Procedure Act	- DETKONGELIGEJUSTIS-OG BEREDSKAPSDEPARTMENT, Ministry of Justice and Public Security, Act of 22 May 1981 No. 25. With subsequent amendments, the latest made by - Act of 21 June 2013 No. 84
Specific range of application of the tool	Audio, video, area and people	Section 216-a (a)
How is the tool defined?	If there is a cause to suspect that one or more criminal acts punishable pursuant to statute by imprisonment for a term exceeding six months have been committed, the police may carry out concealed video surveillance of a public place (also approved in Data protection act - section 40 of the Personal Data Act) if such surveillance will be of substantial significance for the investigation	1) Chapter 15, Section 202 a 2) Section 192
For what types of crime can the tool be used?	If any person is with a cause suspected of committing an act or an attempt at an act that is punishable pursuant to statute by imprisonment for a term of five years or more, or that contravenes sections 90 (genocide), 91 (financial crimes).	Chapter 15, Section 202 b
Does national law allow this tool to be used in cross border cases?	In case of audio surveillance - The court may make an order permitting the police to carry out communications surveillance when any person is with just cause suspected of an act or attempt at an act - please refer to above penal code.	section 216 a para 1
What thresholds must be passed for the use of this tool?	if person violated sections 90 (genocide), 91 (financial crimes). of the Penal Code.	Chapter 15, Section 202 b
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	the video surveillance should not be exceed 4 weeks. It may be extended upon the request	Section 202 a, para 2
What are the rules to be followed for the implementation of this tool?	LEAs	- Section 202 a, para 2 - section 225
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Judicial Court gives permission and local police uses the tool.	Section 216, para 1

Relevant items	Provisions	Sources used
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	1) In order to secure evidence, the prosecuting authority, or in urgent cases a police officer, may close a building or premises, close off a specific area, prohibit the moving or touching of specific objects, or take similar precautions. 2) In case of audio surveillance - Communications surveillance may consist of audio surveillance of conversations or other communications conducted to or from specific telephones, computers or other apparatus for electronic communication which the suspect possesses or which it may be assumed he will use.	1) Section 216 2) section 216 para 3
What ongoing supervision is required for the use of this tool?	The audio/video surveillance should not exceed of 4 weeks at a time. Then Police has to request court to extend this period for another 4 weeks. Court should look in to evidence collected by police in first 4 week period and if evidence is concrete then should allow for another 4 week period. More than 4 weeks period is a breach into human rights of the person (Section 4 of Data Protection Act)	section 216 a para 1
Is there any national case law relating to the use of this tool in cross-border crime cases?	Public Prosecutor.	Section 202 a, para 2
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Undercover / covert operations		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Procedure Act	DETKONGELIGEJUSTIS-OG BEREDSKAPSDEPARTMENT, Ministry of Justice and Public Security, Act of 22 May 1981 No. 25. With subsequent amendments, the latest made by Act of 21 June 2013 No. 84
How is the tool defined?	There is no definition given in the national law. But law says that the court may make an order permitting the police to carry out covert investigation.	section 216-m (1)
For what types of crime can the tool be used?	In the violation of penal code: Participation in military activity in an armed conflict abroad (section 145), Rioting (section 182), trafficking of fire arms (section) 189, serious environmental crime (like polluting air) (section 240) of the Penal Code.	section 216-m (a), (b), ©. Section 145, 182, 189, and 240 of Penal Code link - https://lovdata.no/dokument/NLE/lov/2005-05-20-28/*&#x2a;
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	In the violation of penal code: Participation in military activity in an armed conflict abroad (section 145), Rioting (section 182), trafficking of fire arms (section) 189, serious environmental crime (like polluting air) (section 240) of the Penal Code.	section 216-m (a), (b), ©. Section 145, 182, 189, and 240 of Penal Code link - https://lovdata.no/dokument/NLE/lov/2005-05-20-28/*&#x2a;
What types of stakeholder are involved in the implementation of this tool?	LEAs (A decision concerning video surveillance pursuant to the first paragraph shall be made by the court. Permission shall be given for a specific period which shall not be longer than is strictly necessary and shall not exceed four weeks)	- Section 202 a, para 2 - section 225
Which LEAs can use this tool?	Judicial Court and LEAs	Section 216, para 1
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	It cannot used for more than 4 weeks at a time, as it may have chance to violate the human rights of the person	Section 216-a
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Public Prosecutor	Section 202 a, para 2
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	N/A	
Specific range of application of the tool	N/A	
How is the tool defined?	N/A	

Relevant items	Provisions	Sources used
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	

Source: Author’s own elaboration

Poland

Table 41 – Overview of national rules on investigative tools - Poland

Relevant items	Provisions	Sources used
Controlled Delivery		
Relevant documents (legal and non-legal) that define the functioning of the tool	The usage of this investigative tool is very complex due to the number of authorised bodies (please refer to the question 13 for the details) and different legislation assigned to almost each force/service unit. Due to the large amount of overlapping sources, the above data, definitions, and statistics were based mostly on the available information for the tool usage by the police. Lex generalis (Acts - available in English) 1. Act of 6 April 1990 on the Police, here and later referred as the Act on the Police (Ustawa z dnia 6 kwietnia 1990 r. o Policji). 2. Act of 15 January 2016 amending the Police Act and certain other acts, here and later referred as the "Polish Surveillance Act" ("Ustawa inwigilacyjna" - Ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw). 3. The Penal Code (Ustawa z dnia 6 czerwca 1997 r. Kodeks karny) containing list of criminal activities referred in the above regulations. Lex specialis (ordinances - available in Polish): 4. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 13 marca 2002 r. w sprawie sposobu przeprowadzania i dokumentowania przez Policję czynności operacyjno-rozpoznawczych polegających na dokonaniu w sposób niejawny nabycia, zbycia lub przejęcia przedmiotów pochodzących z przestępstwa, ulegających przypadkowi albo których wytwarzanie, posiadanie, przewożenie lub którymi obrót są zabronione, a także na przyjęciu lub wręczeniu korzyści majątkowej, oraz sposobu przekazywania, przetwarzania i niszczenia materiałów uzyskanych podczas stosowania tych czynności. 5. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 13 marca 2002 r. w sprawie sposobu przeprowadzania i dokumentowania przez Policję niejawnego nadzorowania wytwarzania, przemieszczania, przechowywania i obrotu przedmiotami przestępstwa. Regarding other law-enforcement bodies: please refer to the question 18 for the details.	1. Act of 6 April 1990 on the Police, here and later referred as the Act on the Police (Ustawa z dnia 6 kwietnia 1990 r. o Policji). https://www.policja.pl/ftp/pliki/police_act.pdf 2. Act of 15 January 2016 amending the Police Act and certain other acts, here and later referred as the "Polish Surveillance Act" ("Ustawa inwigilacyjna" - Ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw). https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-REF(2016)036-e 3. The Penal Code (Ustawa z dnia 6 czerwca 1997 r. Kodeks karny) containing list of criminal activities referred in the above regulations. https://www.legislationline.org/download/id/7354/file/Poland_CC_1997_en.pdf 4. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 13 marca 2002 r. w sprawie sposobu przeprowadzania i dokumentowania przez Policję czynności operacyjno-rozpoznawczych polegających na dokonaniu w sposób niejawny nabycia, zbycia lub przejęcia przedmiotów pochodzących z przestępstwa, ulegających przypadkowi albo których wytwarzanie, posiadanie, przewożenie lub którymi obrót są zabronione, a także na przyjęciu lub wręczeniu korzyści majątkowej, oraz sposobu przekazywania, przetwarzania i niszczenia materiałów uzyskanych podczas stosowania tych czynności. http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20020230240 5. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 13 marca 2002 r. w sprawie sposobu przeprowadzania i dokumentowania przez Policję niejawnego nadzorowania wytwarzania, przemieszczania, przechowywania i obrotu przedmiotami przestępstwa. http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20020230239 1. Act of 6 April 1990 on the Police, here and later referred as the Act on the Police (Ustawa z dnia 6 kwietnia 1990 r. o Policji).
How is the tool defined?	<u>Act on the Police (1)</u> : Article 19.	

Relevant items	Provisions	Sources used
	(..) 6. The operational controls are performed confidentially and consist of: 1) extracting and recording the content of conversations carried out using technical resources, including telecommunications networks; 2) extracting and recording images and sounds of people in inside spaces, transport or any non-public places; 3) extracting the content of correspondence, including correspondence exchanged through electronic means of communication; 4) extracting and recording data from data storage media, telecommunications terminal equipment, information and communication systems; 5) gaining access to and checking the contents of mail.	https://www.policja.pl/ftp/pliki/police_act.pdf
For what types of crime can the tool be used?	All of the crime categories listed on the left and series of additional, described in detail in the Penal Code due to their specificity. The full detailed catalogue is provided in the below article of the Act on the Police, and their officially translated references can be found in the Penal Code provided on the right. <u>Act on the Police (1):</u> Article 19. 1. In case of preliminary investigation carried out by the Police to prevent, detect, establish perpetrators and to obtain and record evidence of the perpetrators prosecuted on indictment, of intentional crime: (1) against life, as defined in Articles 148-150 of the Penal Code, (2) defined in Article 134, Article 135 Paragraph 1, Article 136 Paragraph 1, Article 156 Paragraphs 1 and 3, Article 163 Paragraphs 1 and 3, Article 164 Paragraph 1, Article 165 Paragraphs 1 and 3, Article 166, 167, 173 Paragraphs 1 and 3, Article 189, 204 Paragraph 4, Articles 223, 228, 229, 232, 245, 246, 252 Paragraphs 1-3, Articles 253, 258, 269, 280-282, 285 Paragraph 1, Article 286, 296, 299 Paragraphs 1-6 and in Article 310 Paragraphs 1, 2 and 4 of the Penal Code, (3) against economic turnover defined in Article 297-306 of the Penal Code, resulting in property loss or directed against property, if the damage is in excess of the multiple of fifty minimum wages, defined on the basis of separate provisions, (4) Fiscal crimes, if the value of the subject of offence or reduction of public private amount due is in excess of the multiple of fifty minimum wages, defined on the basis of separate provisions, (5) illegal manufacture, possession or turnover in arms, ammunition, explosives, intoxicants, psychotropic substances and their precursors, as well as nuclear and radioactive materials, (6) defined in Article 8 of the Act of 6 June 1997 – Provisions implementing the Penal Code (Dz. U. No 88, item 554, as amended), (7) defined in Article 43-46 of the Act of 1 July 2005 on collection, storage and transplantation of cells, tissues and organs (Dz. U. No 169, item 1411), (8) prosecuted under international contracts and agreements".	1. Act of 6 April 1990 on the Police, here and later referred as the Act on the Police (Ustawa z dnia 6 kwietnia 1990 r. o Policji). - https://www.policja.pl/ftp/pliki/police_act.pdf 2. The Penal Code (Ustawa z dnia 6 czerwca 1997 r. Kodeks karny) containing list of criminal activities referred in the above regulations. - https://www.legislationline.org/download/id/7354/file/Poland_CC_1997_en.pdf
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	Police Commander in Chief, General Public Prosecutor, Voivodship Police Commander, the lower (Sejm) and upper (Senat) chamber of the Parliament. Their detailed roles, depending of the stage of the investigation and other circumstances are included in the below quotation from the Act on the Police: <u>Act on the Police:</u> Article 19. (..) 2. The provision referred to in Paragraph 1 shall be issued by the district court with territorial competence on account of the seat of the Police authority submitting the request. 3. In cases of the utmost urgency, where any delay could result in the loss of information or the obliteration or destruction of the evidence of a crime, the Police Commander in Chief or the Voivodship Police Commander may order, upon a written consent of the competent prosecutor referred to in Paragraph 1, operational control, submitting also a request for resolution in that matter to the district court with territorial competence. Should consent not be granted within 5 days from the day of ordering operational control, the managing authority shall withhold the operational control and perform destruction of materials collected during the control in the presence of a committee to be evidenced by a report. 4. The district court may permit the abandonment of destruction of materials referred to in Paragraph 3, on written request of the Police Commander in Chief or the Voivodship Police Commander, following a written consent of the competent prosecutor, if the materials are	1. Act of 6 April 1990 on the Police, here and later referred as the Act on the Police (Ustawa z dnia 6 kwietnia 1990 r. o Policji). - https://www.policja.pl/ftp/pliki/police_act.pdf

Relevant items	Provisions	Sources used
	evidence or indicate intention to commit crime, which can be detected by way of operational control or preliminary investigation. 5. Should the need arise to order operational control in relation to a suspect or person charged, the request of the Police authority, referred to in Paragraph 1, to order operational control should be accompanied by information about the proceedings against that person. (..) 7. The request of the Police authority, referred to in Paragraph 1, to operational control ordered by the district court, should include in particular: (1) case number and cryptonym, if applicable, (2) description of the crime, stating, if possible, its legal qualification, (3) circumstances justifying the need to perform operational control, including stated or possible ineffectiveness or uselessness of other means, (4) personal data or other data facilitating unambiguous determination of the entity or object subject to operational control, stating the place or procedure for undertaking the control, (5) objective, time and type of operational control referred to in Paragraph 6. 8. Operational control shall be ordered for a period not exceeding 3 months. The District court may, upon written request of the Police Commander in Chief or the Voivodship Police Commander, following a written consent of the competent prosecutor, for a period not exceeding 3 subsequent months, issue a resolution on single extension of operational control, if the reasons for ordering the control have not been established. 9. In justified cases, when new circumstances important to prevent or detect crime or establish perpetrators and obtain evidence of crime appear, the district court may, upon a written request of the Police Commander in Chief, following a written consent of the General Public Prosecutor, issue a resolution on operational control for the period determined also after the periods referred to in Paragraph 8. 10. The provision of Paragraph 7 shall apply to requests referred to in Paragraphs 3, 4, 8 and 9 respectively. The court, prior to issuing the resolution referred to in Paragraphs 3, 4, 8 and 9, may wish to see the materials justifying the request, which were collected during operational control ordered for that case. 11. Requests referred to in Paragraphs 1, 3-5, 8 and 9 shall be examined by the district court individually, at the same time court proceedings relating to examination of the requests should be performed under conditions foreseen for submission, storage and provision of secret information and adequate application of the regulations issued pursuant to Article 181 § 2 of the Code of Criminal Procedure. The court sitting may be attended only by a prosecutor and a representative of the Police authority requesting the order of operational control. 12. Entities carrying out telecommunications activity and entities providing postal services shall ensure, at their own expense, technical and organisational conditions facilitating the operational control carried out by the Police. 13. Operational control should be completed immediately when the causes of its institution no longer exist, at the latest, however, upon the expiry date. 14. The Police authority referred to in Paragraph 1 shall notify the competent prosecutor about the results of operational control upon its completion, and upon his request also about the course of control. 15. Should evidence be obtained facilitating the institution of criminal proceedings or significant to the criminal proceedings in progress, the Police Commander in Chief or the Voivodship Police Commander shall provide the competent prosecutor with any and all materials collected during operational control, if necessary, with the request for institution of criminal proceedings. Provisions of Article 393 Paragraph 1 first sentence of the Code of Criminal Proceedings shall apply accordingly to proceedings before a court in respect to the materials. 16. The person subject to operational control shall not be provided with materials collected during the control. The provision is not in violation of the rights under Article 321 of the Code of Criminal Proceedings. 17. Materials collected during operational control, which do not include evidence facilitating the institution of criminal proceedings, shall be stored after the conclusion of control for the period of 2 months. They shall then be destroyed in the presence of a committee and the process evidenced in a report. The destruction of materials shall be ordered by the Police authority, which requested the operational control. 18. Procedures referred to in Paragraphs 1-11 shall not apply, if operational control is carried out following a written consent of the sender or recipient of information. 19. In cases referred to in Paragraph 18, operational control is ordered by the Police authority competent preliminary investigation of the case. 20. The ruling of the court concerning operational control referred to in Paragraphs 1, 3, 8 and 9, and the ruling concerning abandonment of destruction of materials collected during operational control referred to in Paragraph 4 may be appealed against by the Police authority,	

Relevant items	Provisions	Sources used
	which requested such ruling. Provisions of the Code of Criminal Proceedings shall apply accordingly to the appeal. 21. The Minister competent for internal matters, upon consultation with the Minister of Justice and the Minister competent for communications, shall determine, by way of ordinance, mode of record of operational control and storage and submission of requests and orders, as well as storage, submission, processing and destruction of materials obtained during control, taking account of the necessity to ensure secret character of measures taken and materials obtained, and models of forms and registers used. 22. The General Public Prosecutor shall provide the lower (Sejm) and upper (Senat) chamber of the Parliament with information about the activity defined in Paragraphs 1-21, including information and data referred to in Article 20 (3).	
Which LEAs can use this tool?	+ Police + Border Control (<i>Straż Graniczna</i>) + Military Police (<i>Żandarmeria Wojskowa</i>) + Officers of the Revenue Intelligence unit of the Tax Office (<i>funkcjonariusze wywiadu skarbowego Urzędu Skarbowego</i>) + Special Services (<i>Służby Specjalne</i>): - Internal Security Agency / <i>Agencja Bezpieczeństwa Wewnętrznego (ABW)</i> - Central Anticorruption Bureau / <i>Centralne Biuro Antykorupcyjne (CBA)</i> - Military Counterintelligence Service / <i>Służba Kontrwywiadu Wojskowego (SKW)</i> - Military Intelligence Service / <i>Służba Wywiadu Wojskowego (SWW)</i>	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool?	The detailed process of granting the authorisation is described in the Act on the Police: <u>Act on the Police:</u> Article 19. (..) 2. The provision referred to in Paragraph 1 shall be issued by the district court with territorial competence on account of the seat of the Police authority submitting the request. 3. In cases of the utmost urgency, where any delay could result in the loss of information or the obliteration or destruction of the evidence of a crime, the Police Commander in Chief or the Voivodship Police Commander may order, upon a written consent of the competent prosecutor referred to in Paragraph 1, operational control, submitting also a request for resolution in that matter to the district court with territorial competence. Should consent not be granted within 5 days from the day of ordering operational control, the managing authority shall withhold the operational control and perform destruction of materials collected during the control in the presence of a committee to be evidenced by a report. 4. The district court may permit the abandonment of destruction of materials referred to in Paragraph 3, on written request of the Police Commander in Chief or the Voivodship Police Commander, following a written consent of the competent prosecutor, if the materials are evidence or indicate intention to commit crime, which can be detected by way of operational control or preliminary investigation. 5. Should the need arise to order operational control in relation to a suspect or person charged, the request of the Police authority, referred to in Paragraph 1, to order operational control should be accompanied by information about the proceedings against that person. (..) 7. The request of the Police authority, referred to in Paragraph 1, to operational control ordered by the district court, should include in particular: (1) case number and cryptonym, if applicable, (2) description of the crime, stating, if possible, its legal qualification, (3) circumstances justifying the need to perform operational control, including stated or possible ineffectiveness or uselessness of other means, (4) personal data or other data facilitating unambiguous determination of the entity or object subject to operational control, stating the place or procedure for undertaking the control, (5) objective, time and type of operational control referred to in Paragraph 6. 8. Operational control shall be ordered for a period not exceeding 3 months. The District court may, upon written request of the Police Commander in Chief or the Voivodship Police Commander, following a written consent of the competent prosecutor, for a period not exceeding	

Relevant items	Provisions	Sources used
	3 subsequent months, issue a resolution on single extension of operational control, if the reasons for ordering the control have not been established. 9. In justified cases, when new circumstances important to prevent or detect crime or establish perpetrators and obtain evidence of crime appear, the district court may, upon a written request of the Police Commander in Chief, following a written consent of the General Public Prosecutor, issue a resolution on operational control for the period determined also after the periods referred to in Paragraph 8. 10. The provision of Paragraph 7 shall apply to requests referred to in Paragraphs 3, 4, 8 and 9 respectively. The court, prior to issuing the resolution referred to in Paragraphs 3, 4, 8 and 9, may wish to see the materials justifying the request, which were collected during operational control ordered for that case. 11. Requests referred to in Paragraphs 1, 3-5, 8 and 9 shall be examined by the district court individually, at the same time court proceedings relating to examination of the requests should be performed under conditions foreseen for submission, storage and provision of secret information and adequate application of the regulations issued pursuant to Article 181 § 2 of the Code of Criminal Procedure. The court sitting may be attended only by a prosecutor and a representative of the Police authority requesting the order of operational control. 12. Entities carrying out telecommunications activity and entities providing postal services shall ensure, at their own expense, technical and organisational conditions facilitating the operational control carried out by the Police. 13. Operational control should be completed immediately when the causes of its institution no longer exist, at the latest, however, upon the expiry date. 14. The Police authority referred to in Paragraph 1 shall notify the competent prosecutor about the results of operational control upon its completion, and upon his request also about the course of control. 15. Should evidence be obtained facilitating the institution of criminal proceedings or significant to the criminal proceedings in progress, the Police Commander in Chief or the Voivodship Police Commander shall provide the competent prosecutor with any and all materials collected during operational control, if necessary, with the request for institution of criminal proceedings. Provisions of Article 393 Paragraph 1 first sentence of the Code of Criminal Proceedings shall apply accordingly to proceedings before a court in respect to the materials. 16. The person subject to operational control shall not be provided with materials collected during the control. The provision is not in violation of the rights under Article 321 of the Code of Criminal Proceedings. 17. Materials collected during operational control, which do not include evidence facilitating the institution of criminal proceedings, shall be stored after the conclusion of control for the period of 2 months. They shall then be destroyed in the presence of a committee and the process evidenced in a report. The destruction of materials shall be ordered by the Police authority, which requested the operational control. 18. Procedures referred to in Paragraphs 1-11 shall not apply, if operational control is carried out following a written consent of the sender or recipient of information. 19. In cases referred to in Paragraph 18, operational control is ordered by the Police authority competent preliminary investigation of the case. 20. The ruling of the court concerning operational control referred to in Paragraphs 1, 3, 8 and 9, and the ruling concerning abandonment of destruction of materials collected during operational control referred to in Paragraph 4 may be appealed against by the Police authority, which requested such ruling. Provisions of the Code of Criminal Proceedings shall apply accordingly to the appeal. 21. The Minister competent for internal matters, upon consultation with the Minister of Justice and the Minister competent for communications, shall determine, by way of ordinance, mode of record of operational control and storage and submission of requests and orders, as well as storage, submission, processing and destruction of materials obtained during control, taking account of the necessity to ensure secret character of measures taken and materials obtained, and models of forms and registers used. 22. The General Public Prosecutor shall provide the lower (Sejm) and upper (Senat) chamber of the Parliament with information about the activity defined in Paragraphs 1-21, including information and data referred to in Article 20 (3).	
What ongoing supervision is required for the use of this tool?	There is no "requirement" but according to the Act on the Police: <u>Act on the Police:</u> Article 19. 14. The Police authority referred to in Paragraph 1 shall notify the competent prosecutor about the results of operational control upon its completion, and upon his request also about the	

Relevant items	Provisions	Sources used
Is there any national case law relating to the use of this tool in cross-border crime cases?	course of control. N/A	
Data available on the number of times this tool has been used for SOC cases	Usage number of this investigative tool by authorised bodies during period included in available data is very low (i.e. 0 in 2013).	1. Use of the information gathered by operational means by the courts of the first instance (<i>Korzystanie w postępowaniu karnym przez sądy pierwszej instancji z informacji zebranych operacyjnie</i>), page 57 (available in Polish): https://iws.gov.pl/wp-content/uploads/2018/08/IWS_Szumi%C5%82o-Kulczycka-D._._-z-inf.-zebranych-operacyjnie.pdf
Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	[Only implemented national regulations based on the EU law were taken into account] 1. Order of the Chief of Police No. 1355 of December 2007 on the methods and forms of organizing and conducting the police hot pursuits and organised activities pursuit and procedures for conducting cross-border / hot pursuit of individual neighbouring countries, here and later referred as "Order on the hot pursuit" (<i>Zarządzenie Nr 1355 Komendanta Głównego Policji z dnia 20 grudnia 2007 r. w sprawie metod i form organizowania i prowadzenia przez Policję pościgów i zorganizowanych działań pościgowych</i> , based on the Act on the Police).	- Order of the Chief of Police No. 1355 of December 2007 on the methods and forms of organizing and conducting the police hot pursuits and organised activities pursuit and procedures for conducting cross-border / hot pursuit of individual neighbouring countries, here and later referred as "Order on the hot pursuit" (<i>Zarządzenie Nr 1355 Komendanta Głównego Policji z dnia 20 grudnia 2007 r. w sprawie metod i form organizowania i prowadzenia przez Policję pościgów i zorganizowanych działań pościgowych</i>, based on the Act on the Police). https://www.infor.pl/akt-prawny/U27.2008.001.0000001,zarzadzenie-nr-1355-komendanta-glownego-policji-w-sprawie-metod-i-form-organizowania-i-prowadzenia-przez-policje-poscigow-i-zorganizowanych-dzialan-poscigowych.html
How is the tool defined?	<u>Order on the hot pursuit:</u> § 3. (..) 5) hot pursuit - a pursuit or organised pursuit activities carried out on the territory of at least two countries or - in the case of taking over the pursuit from officers of another country - on the territory of the Republic of Poland;	- Order of the Chief of Police No. 1355 of December 2007 on the methods and forms of organizing and conducting the police hot pursuits and organised activities pursuit and procedures for conducting cross-border / hot pursuit of individual neighbouring countries, here and later referred as "Order on the hot pursuit" (<i>Zarządzenie Nr 1355 Komendanta Głównego Policji z dnia 20 grudnia 2007 r. w sprawie metod i form organizowania i prowadzenia przez Policję pościgów i zorganizowanych działań pościgowych</i>, based on the Act on the Police). https://www.infor.pl/akt-prawny/U27.2008.001.0000001,zarzadzenie-nr-1355-komendanta-glownego-policji-w-sprawie-metod-i-form-organizowania-i-prowadzenia-przez-policje-poscigow-i-zorganizowanych-dzialan-poscigowych.html
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	Order on the hot pursuit: § 33. On duty officer of the Police Headquarters: 1) coordinates organised pursuit activities until the appointment of a police operation commander; 2) collects and exchanges information about the course of pursuit activities with the competent duty officers of the voivodeship police headquarters; 3) exchanges information with officers of competent authorities of other countries in justified cases. § 34. On duty officer of the provincial police headquarters: 1) directs to organised pursuit activities the forces and resources from other organisational units of the Police in the voivodeship, if the activities carried out by the regional police headquarters do not predict the achievement of the goal; 2) coordinates the activities of the regional police headquarters until the police operation commander is appointed by the provisional police commander; 3) informs on an ongoing basis about the course of the activities of the provincial police commander and the duty officer of the Police Headquarters and, depending on the situation, on duty of neighbouring provincial Police headquarters and co-operating duty services; 4) agree with the press spokesman of the provincial police headquarters on the legitimacy of providing the mass media with a message informing about the incident and the organised pursuit activities; 5) in justified cases, asks the officer on duty of the Police Headquarters for assistance by other provincial police headquarters. § 35. On duty officer at the regional police headquarters, after receiving information about the domestic pursuit:	- Order of the Chief of Police No. 1355 of December 2007 on the methods and forms of organizing and conducting the police hot pursuits and organised activities pursuit and procedures for conducting cross-border / hot pursuit of individual neighbouring countries, here and later referred as "Order on the hot pursuit" (<i>Zarządzenie Nr 1355 Komendanta Głównego Policji z dnia 20 grudnia 2007 r. w sprawie metod i form organizowania i prowadzenia przez Policję pościgów i zorganizowanych działań pościgowych</i>, based on the Act on the Police). https://www.infor.pl/akt-prawny/U27.2008.001.0000001,zarzadzenie-nr-1355-komendanta-glownego-policji-w-sprawie-metod-i-form-organizowania-i-prowadzenia-przez-policje-poscigow-i-zorganizowanych-dzialan-poscigowych.html

Relevant items	Provisions	Sources used
	1) notifies policemen serving in the area of organised pursuit activities about the incident; 2) directs forces and support measures and organizes a blockade; 3) directs policemen to the place of organised pursuit activities in order to collect additional information about the chased person, the means of transport used, the direction of his escape, and to establish witnesses of the incident, as well as to secure the scene of the incident; 4) informs about the incident and actions taken by the head of the Police organisational unit and the officer on duty of the superior Police organisational unit; 5) if required, the nature of the incident calls the specialised emergency services to the place of the incident; 6) notifies other organisational units of the Police and Border Guard posts about the need to organize a blockade, and in the event that the prosecuted persons may leave the area subordinate to an organisational unit of the Police, inform these units about the type and number of involved forces and provide them with data enabling unambiguous identification of police officers and vehicles used for pursuit, in particular radio code names, registration numbers, tactical signs of police cars; 7) directs organised pursuit activities until the appointment of the commander of the police action or operation.	
Which LEAs can use this tool?	Police	- Order of the Chief of Police No. 1355 of December 2007 on the methods and forms of organizing and conducting the police hot pursuits and organised activities pursuit and procedures for conducting cross-border / hot pursuit of individual neighbouring countries, here and later referred as "Order on the hot pursuit" (<i>Zarządzenie Nr 1355 Komendanta Głównego Policji z dnia 20 grudnia 2007 r. w sprawie metod i form organizowania i prowadzenia przez Policję pościgów i zorganizowanych działań pościgowych, based on the Act on the Police</i>). https://www.infor.pl/akt-prawny/U27.2008.001.0000001,zarzadzenie-nr-1355-komendanta-glownego-policji-w-sprawie-metod-i-form-organizowania-i-prowadzenia-przez-policje-poscigow-i-zorganizowanych-dzialan-poscigowych.html
What are the rules to be followed for the implementation of this tool?	Developed in the "Questionnaire for completion by national experts" during the "Study on paving the way for future policy initiatives in the field of fight against organised crime - effectiveness of specific criminal law measures targeting organised crime" (1) based on the Order on the hot pursuit (2): The rules are as follow: 1) when conducting cross-border pursuits exchange of information takes place via the duty service of relevant organisational units of the Police, 2) when conducting cross-border pursuit police provide information promptly and regularly about the situation on duty service of organisational unit of the Police or the police commander of incident or operations during a pursuit conducted on Polish territory or the competent authority of the Member in the course of the pursuit conducted outside Polish territory, 3) on the instructions of duty service of organisational unit of the Police or the police commander police officers take over the pursuit from the state officials who run hot pursuit on Polish territory, as well as the person apprehended along with received items, 4) police officers who are conducting a hot pursuit are obliged to comply with the provisions of law and orders of the competent authorities of the State in the territory of which they are conducting hot pursuit, to show their official identity card to any request of officers of the competent authority of the State in the territory of which they are conducting hot pursuit, 5) after the pursuit the police officers submit to the competent authority of the State in the territory of which they are conducting hot pursuit, a report on the activities they carried out, 6) in the case of crossing the state border by the police officers conducting national hot pursuit, the duty service of the organisational unit of the Police passes the superior organisational unit of the Police information which allow their identification, 7) after receiving information about the cross-border pursuit conducted by the officers of another State on the territory of the Republic of Polish, the duty service of the organisational unit of the Police directs the forces and technical means to immediately take over the pursuit and communicate to the superior duty service of the organisational unit of the Police identifiable information about officers and policemen taking over hot pursuit which allow their identification. The cross-border pursuit is conducted with a framework of the police action or operation, from time of initial information about this pursuit until the appointment of the incident or operations commander. All activities related to the conducting hot pursuit are coordinated by the duty service officer of the Police provincial command.	- Order of the Chief of Police No. 1355 of December 2007 on the methods and forms of organizing and conducting the police hot pursuits and organised activities pursuit and procedures for conducting cross-border / hot pursuit of individual neighbouring countries, here and later referred as "Order on the hot pursuit" (<i>Zarządzenie Nr 1355 Komendanta Głównego Policji z dnia 20 grudnia 2007 r. w sprawie metod i form organizowania i prowadzenia przez Policję pościgów i zorganizowanych działań pościgowych, based on the Act on the Police</i>). https://www.infor.pl/akt-prawny/U27.2008.001.0000001,zarzadzenie-nr-1355-komendanta-glownego-policji-w-sprawie-metod-i-form-organizowania-i-prowadzenia-przez-policje-poscigow-i-zorganizowanych-dzialan-poscigowych.html
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	In two cases: Order on the hot pursuit: 14. In the event of a direct or oral request to stop a cross-border pursuit by phone, the request should be immediately confirmed in writing and sent to the competent authority of the state whose officers conducted the pursuit in the territory of the Republic of Poland.	Order of the Chief of Police No. 1355 of December 2007 on the methods and forms of organizing and conducting the police hot pursuits and organised activities pursuit and procedures for conducting cross-border / hot pursuit of individual neighbouring countries, here and later referred as "Order on the hot pursuit" (<i>Zarządzenie Nr 1355 Komendanta Głównego Policji z dnia 20 grudnia 2007 r. w sprawie metod i form</i>

Relevant items	Provisions	Sources used
	23. A policeman shall also interrupt a cross-border pursuit upon the request of a representative of a competent authority of the state on whose territory the cross-border pursuit is continued.	<i>organizowania i prowadzenia przez Policję pościgów i zorganizowanych działań pościgowych, based on the Act on the Police).</i> https://www.infor.pl/akt-prawny/U27.2008.001.0000001,zarządzenie-nr-1355-komendanta-glownego-policji-w-sprawie-metod-i-form-organizowania-i-prowadzenia-przez-policje-poscigow-i-zorganizowanych-dzialan-poscigowych.html
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Developed in the "Questionnaire for completion by national experts" during the "Study on paving the way for future policy initiatives in the field of fight against organised crime - effectiveness of specific criminal law measures targeting organised crime" (1) based on the Order on the hot pursuit (2): The range the information forwarded by the duty service officer of the Police provincial command includes in particular: 1) the cause of taking up cross-border / hot pursuit, 2) the number of persons pursued, their description, characteristics, such as dress, behaviour, owned by them hazardous items 3) the number, type and characteristics of the means of transportation used by the pursued person, such as brand, type and colour of the vehicle, the registration number and other distinctive characteristics, 4) the direction of pursued persons' movement, the officers' positions conducting cross-border hot pursuit, such as road signs, city name and other important information, 5) the number of police officers conducting cross-border hot pursuit, the identity of their commander, characteristics of clothing, such as: full service uniforms or some of their elements, owned weapons, technology and communications means, 6) the expected time and place taking over the pursuit, 7) the expected time and place of crossing of the state border, 8) the number, type and characteristics of the means of transportation used by the police officers, such as brand, type and colour of the vehicle, the registration number and other distinctive characteristics, 9) the features of the officers appointed to take over the cross-border pursuit which allow their identification.	- Order of the Chief of Police No. 1355 of December 2007 on the methods and forms of organizing and conducting the police hot pursuits and organised activities pursuit and procedures for conducting cross-border / hot pursuit of individual neighbouring countries, here and later referred as "Order on the hot pursuit" (Zarządzenie Nr 1355 Komendanta Głównego Policji z dnia 20 grudnia 2007 r. w sprawie metod i form organizowania i prowadzenia przez Policję pościgów i zorganizowanych działań pościgowych, based on the Act on the Police). - https://www.infor.pl/akt-prawny/U27.2008.001.0000001,zarządzenie-nr-1355-komendanta-glownego-policji-w-sprawie-metod-i-form-organizowania-i-prowadzenia-przez-policje-poscigow-i-zorganizowanych-dzialan-poscigowych.html
What ongoing supervision is required for the use of this tool?	<u>Order on the hot pursuit:</u> § 33. On duty officer of the Police Headquarters: 1) coordinates organised pursuit activities until the appointment of a police operation commander; 2) collects and exchanges information about the course of pursuit activities with the competent duty officers of the voivodeship police headquarters; 3) exchanges information with officers of competent authorities of other countries in justified cases. § 34. On duty officer of the provincial police headquarters: 1) directs to organised pursuit activities the forces and resources from other organisational units of the Police in the voivodeship, if the activities carried out by the regional police headquarters do not predict the achievement of the goal; 2) coordinates the activities of the regional police headquarters until the police operation commander is appointed by the provisional police commander; 3) informs on an ongoing basis about the course of the activities of the provincial police commander and the duty officer of the Police Headquarters and, depending on the situation, on duty of neighbouring provincial Police headquarters and co-operating duty services; 4) agree with the press spokesman of the provincial police headquarters on the legitimacy of providing the mass media with a message informing about the incident and the organised pursuit activities; 5) in justified cases, asks the officer on duty of the Police Headquarters for assistance by other provincial police headquarters. § 35. On duty officer at the regional police headquarters, after receiving information about the domestic pursuit: 1) notifies policemen serving in the area of organised pursuit activities about the incident; 2) directs forces and support measures and organizes a blockade; 3) directs policemen to the place of organised pursuit activities in order to collect additional information about the chased person, the means of transport used, the direction of his escape, and to establish witnesses of the incident, as well as to secure the scene of the incident; 4) informs about the incident and actions taken by the head of the Police organisational unit and the officer on duty of the superior Police organisational unit;	- Order of the Chief of Police No. 1355 of December 2007 on the methods and forms of organizing and conducting the police hot pursuits and organised activities pursuit and procedures for conducting cross-border / hot pursuit of individual neighbouring countries, here and later referred as "Order on the hot pursuit" (Zarządzenie Nr 1355 Komendanta Głównego Policji z dnia 20 grudnia 2007 r. w sprawie metod i form organizowania i prowadzenia przez Policję pościgów i zorganizowanych działań pościgowych, based on the Act on the Police). - https://www.infor.pl/akt-prawny/U27.2008.001.0000001,zarządzenie-nr-1355-komendanta-glownego-policji-w-sprawie-metod-i-form-organizowania-i-prowadzenia-przez-policje-poscigow-i-zorganizowanych-dzialan-poscigowych.html

Relevant items	Provisions	Sources used
	5) if required, the nature of the incident calls the specialised emergency services to the place of the incident; 6) notifies other organisational units of the Police and Border Guard posts about the need to organize a blockade, and in the event that the prosecuted persons may leave the area subordinate to an organisational unit of the Police, inform these units about the type and number of involved forces and provide them with data enabling unambiguous identification of police officers and vehicles used for pursuit, in particular radio code names, registration numbers, tactical signs of police cars; 7) directs organised pursuit activities until the appointment of the commander of the police action or operation.	
Is there any national case law relating to the use of this tool in cross-border crime cases?	No national case law related directly to the international hot pursuits are available online. Limited media coverage available (please see example in the attached source)	- https://www.policja.pl/pol/aktualnosci/80658,Poscig-przez-granice.html - https://www.igryfino.pl/wiadomosci/31052,oblawa-na-zlodzieja-samochodow-poscig-transgraniczny
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	Or quotations in this section are from below legislature: 1. Act on the Crown Witness (Ustawa z dnia 25 czerwca 1997 r. o świadku koronnym).	- Act on the Crown Witness (Ustawa z dnia 25 czerwca 1997 r. o świadku koronnym). - http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19971140738
How is the tool defined?	Article 14. [Crown witness protection program] 1. In the event of a threat to the life or health of a crown witness or the person closest to him within the meaning of the provisions of the Penal Code, they may be subject to personal protection, as well as obtain assistance in changing their place of stay or employment, and in particularly justified cases, they may be issued with documents enabling personal data other than their own, including those entitling them to cross the state border, as well as they may obtain other forms of assistance, in particular, a surgical procedure that removes characteristic elements of the appearance or plastic surgery.	- Act on the Crown Witness (Ustawa z dnia 25 czerwca 1997 r. o świadku koronnym). - http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19971140738
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	Art. 16. [Application for protection] 1. Covering an adult with protection or assistance referred to in Art.14, is subject to the submission of a written commitment by that person to the Commander of the Central Investigation Bureau of the Police or the Director General of the Prison Service to: 1) compliance with the rules and recommendations regarding the protection granted, and 2) performing obligations under the Act and resulting from final judgments and decisions - in the case of using the protection or assistance consisting in changing the place of stay or issuing the documents referred to in art. 14 sec. 1. 2. (repealed). Art. 17. [Order on covering a crown witness with protection] 1. The application of the protection or assistance referred to in Art. 14, the public prosecutor issues an order at the request of a witness from the crown, the suspect, who has met the conditions provided for in Art. 3 sec. 1, or the person closest to them within the meaning of the provisions of the Penal Code. 2. With regard to personal protection, at the request of a crown witness or a person closest to him within the meaning of the provisions of the Penal Code, serving a sentence of imprisonment or detained in prisons or detention centres, the prosecutor issues a decision on granting personal protection, which is carried out by the Director General The Prison Service. 3. The public prosecutor's decision to provide protection or assistance to the persons referred to in para. 1 or 2, may also be issued ex officio - with the consent of these persons. 4. The decision on the application of protection or assistance referred to in para. 1-3 may be appealed.	- Act on the Crown Witness (Ustawa z dnia 25 czerwca 1997 r. o świadku koronnym). - http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19971140738
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	Article 14. [Crown witness protection program] 1. In the event of a threat to the life or health of a crown witness or the person closest to him within the meaning of the provisions of the Penal Code, they may be subject to personal protection, as well as obtain assistance in changing their place of stay or employment, and in particularly justified cases, they may be issued with documents enabling personal data other than	- Act on the Crown Witness (Ustawa z dnia 25 czerwca 1997 r. o świadku koronnym). - http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19971140738

Relevant items	Provisions	Sources used
	their own, including those entitling them to cross the state border, as well as they may obtain other forms of assistance, in particular, a surgical procedure that removes characteristic elements of the appearance or plastic surgery.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	The rules and restrictions are included in the article 14 (quoted above)	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Art. 16. [Application for protection] 1. Covering an adult with protection or assistance referred to in Art.14, is subject to the submission of a written commitment by that person to the Commander of the Central Investigation Bureau of the Police or the Director General of the Prison Service to: 1) compliance with the rules and recommendations regarding the protection granted, and 2) performing obligations under the Act and resulting from final judgments and decisions - in the case of using the protection or assistance consisting in changing the place of stay or issuing the documents referred to in art. 14 sec. 1. 2. (repealed). Art. 17. [Order on covering a crown witness with protection] 1. The application of the protection or assistance referred to in Art. 14, the public prosecutor issues an order at the request of a witness from the crown, the suspect, who has met the conditions provided for in Art. 3 sec. 1, or the person closest to them within the meaning of the provisions of the Penal Code. 2. With regard to personal protection, at the request of a crown witness or a person closest to him within the meaning of the provisions of the Penal Code, serving a sentence of imprisonment or detained in prisons or detention centres, the prosecutor issues a decision on granting personal protection, which is carried out by the Director General The Prison Service. 3. The public prosecutor's decision to provide protection or assistance to the persons referred to in para. 1 or 2, may also be issued ex officio - with the consent of these persons. 4. The decision on the application of protection or assistance referred to in para. 1-3 may be appealed.	- Act on the Crown Witness (Ustawa z dnia 25 czerwca 1997 r. o świadku koronnym). http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19971140738
What ongoing supervision is required for the use of this tool?	Art. 16. [Application for protection] 1. Covering an adult with protection or assistance referred to in Art.14, is subject to the submission of a written commitment by that person to the Commander of the Central Investigation Bureau of the Police or the Director General of the Prison Service to: 1) compliance with the rules and recommendations regarding the protection granted, and 2) performing obligations under the Act and resulting from final judgments and decisions - in the case of using the protection or assistance consisting in changing the place of stay or issuing the documents referred to in art. 14 sec. 1. 2. (repealed). Art. 17. [Order on covering a crown witness with protection] 1. The application of the protection or assistance referred to in Art. 14, the public prosecutor issues an order at the request of a witness from the crown, the suspect, who has met the conditions provided for in Art. 3 sec. 1, or the person closest to them within the meaning of the provisions of the Penal Code. 2. With regard to personal protection, at the request of a crown witness or a person closest to him within the meaning of the provisions of the Penal Code, serving a sentence of imprisonment or detained in prisons or detention centres, the prosecutor issues a decision on granting personal protection, which is carried out by the Director General The Prison Service. 3. The public prosecutor's decision to provide protection or assistance to the persons referred to in para. 1 or 2, may also be issued ex officio - with the consent of these persons. 4. The decision on the application of protection or assistance referred to in para. 1-3 may be appealed.	- Act on the Crown Witness (Ustawa z dnia 25 czerwca 1997 r. o świadku koronnym). http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19971140738
Is there any national case law relating to the use of this tool in cross-border crime cases?	The most famous use of the "crown" witness protection programme in Poland was in case of "Masa" - a former gang member of "Pruszków". The subject was well covered in the local media.	https://polandin.com/37230079/saga-of-former-gangster-starts-new-chapter
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	Article 14. [Crown witness protection program] 1. In the event of a threat to the life or health of a crown witness or the person closest to him within the meaning of the provisions of the Penal Code, they may be subject to personal protection, as well as obtain assistance in changing their place of stay or employment, and in particularly justified cases, they may be issued with documents enabling personal data other than their own, including those entitling them to cross the state border, as well as they may obtain other forms of assistance, in particular, a surgical procedure that removes characteristic elements of the appearance or plastic surgery.	- Act on the Crown Witness (Ustawa z dnia 25 czerwca 1997 r. o świadku koronnym). http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19971140738
Surveillance		

Relevant items	Provisions	Sources used
Relevant documents (legal and non-legal) that define the functioning of the tool	Internal comments: A. Please bear in mind that so-called 2016 Polish Surveillance Act amending the Act on the Police and certain other Acts caused great controversy and has become one of the most discussed topics in the media. These regulations are currently under investigation of European Court of Human Rights as per request of the Polish Ombudsman. B. The usage of the term 'Surveillance' is quite general in Polish legislature and is already containing some of the investigative tools grouped separately in this survey (i.e. Controlled Delivery). Therefore the answers might be similar as in the sections dedicated to those tools. C. The usage of this investigative tool is very complex due to the number of authorised bodies and different legislation assigned to almost each force/service unit. Due to the large amount of overlapping sources, presented data, definitions, and statistics were based mostly on the available information for the tool usage by the police. Regarding the police: Lex generalis (Acts - available in English) 1. Act of 6 April 1990 on the Police, here and later referred as the Act on the Police (Ustawa z dnia 6 kwietnia 1990 r. o Policji). 2. Act of 15 January 2016 amending the Police Act and certain other acts, here and later referred as the Polish Surveillance Act ("Ustawa inwigilacyjna" - Ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw). 3. The Penal Code (Ustawa z dnia 6 czerwca 1997 r. Kodeks karny) containing list of criminal activities referred in the above regulations. Lex specialis (ordinances - available in Polish): 4. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 13 marca 2002 r. w sprawie sposobu przeprowadzania i dokumentowania przez Policję czynności operacyjno-rozpoznawczych polegających na dokonaniu w sposób niejawną nabycia, zbycia lub przejęcia przedmiotów pochodzących z przestępstwa, ulegających przypadkowi albo których wytwarzanie, posiadanie, przewożenie lub którymi obrót są zabronione, a także na przyjęciu lub wręczeniu korzyści majątkowej, oraz sposobu przekazywania, przetwarzania i niszczenia materiałów uzyskanych podczas stosowania tych czynności. 5. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 13 marca 2002 r. w sprawie sposobu przeprowadzania i dokumentowania przez Policję niejawnego nadzorowania wytwarzania, przemieszczania, przechowywania i obrotu przedmiotami przestępstwa.	1. Act of 6 April 1990 on the Police, here and later referred as the Act on the Police (Ustawa z dnia 6 kwietnia 1990 r. o Policji). https://www.policja.pl/ftp/pliki/police_act.pdf 2. Act of 15 January 2016 amending the Police Act and certain other acts, here and later referred as the "Polish Surveillance Act" ("Ustawa inwigilacyjna" - Ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw). https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-REF(2016)036-e 3. The Penal Code (Ustawa z dnia 6 czerwca 1997 r. Kodeks karny) containing list of criminal activities referred in the above regulations. https://www.legislationline.org/download/id/7354/file/Poland_CC_1997_en.pdf 4. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 13 marca 2002 r. w sprawie sposobu przeprowadzania i dokumentowania przez Policję czynności operacyjno-rozpoznawczych polegających na dokonaniu w sposób niejawną nabycia, zbycia lub przejęcia przedmiotów pochodzących z przestępstwa, ulegających przypadkowi albo których wytwarzanie, posiadanie, przewożenie lub którymi obrót są zabronione, a także na przyjęciu lub wręczeniu korzyści majątkowej, oraz sposobu przekazywania, przetwarzania i niszczenia materiałów uzyskanych podczas stosowania tych czynności. http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20020230240 5. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 13 marca 2002 r. w sprawie sposobu przeprowadzania i dokumentowania przez Policję niejawnego nadzorowania wytwarzania, przemieszczania, przechowywania i obrotu przedmiotami przestępstwa. http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20020230239
Specific range of application of the tool	<u>Act on the Police (1):</u> Article 19. (..) 6. The operational controls are performed confidentially and consist of: 1) extracting and recording the content of conversations carried out using technical resources, including telecommunications networks; 2) extracting and recording images and sounds of people in inside spaces, transport or any non-public places; 3) extracting the content of correspondence, including correspondence exchanged through electronic means of communication; 4) extracting and recording data from data storage media, telecommunications terminal equipment, information and communication systems; 5) gaining access to and checking the contents of mail.	- Act of 6 April 1990 on the Police, here and later referred as the Act on the Police (Ustawa z dnia 6 kwietnia 1990 r. o Policji). https://www.policja.pl/ftp/pliki/police_act.pdf
How is the tool defined?	N/A	N/A
For what types of crime can the tool be used?	All of the crime categories listed on the left and series of additional, described in detail in the Penal Code due to their specificity. The full detailed catalogue is provided in the below article of the Act on the Police, and their officially translated references can be found in the Penal Code provided on the right. <u>Act on the Police (1):</u> Article 19. 1. In case of preliminary investigation carried out by the Police to prevent, detect, establish perpetrators and to obtain and record evidence of the perpetrators prosecuted on indictment, of intentional crime: (1) against life, as defined in Articles 148-150 of the Penal Code, (2) defined in Article 134, Article 135 Paragraph 1, Article 136 Paragraph 1, Article 156 Paragraphs 1 and 3, Article 163 Paragraphs 1 and 3, Article 164 Paragraph 1, Article 165 Paragraphs 1 and 3, Article 166, 167, 173 Paragraphs 1 and 3, Article 189, 204 Paragraph 4, Articles 223, 228, 229, 232, 245, 246, 252 Paragraphs 1-3, Articles 253, 258, 269, 280-282, 285 Paragraph 1, Article 286, 296, 299 Paragraphs 1-6 and in Article 310 Paragraphs 1, 2 and 4 of the Penal Code, (3) against economic turnover defined in Article 297-306 of the Penal Code, resulting in property loss or directed against property, if the damage is in excess of the multiple of fifty minimum wages, defined on the basis of separate provisions,	- Act of 6 April 1990 on the Police, here and later referred as the Act on the Police (Ustawa z dnia 6 kwietnia 1990 r. o Policji). https://www.policja.pl/ftp/pliki/police_act.pdf

Relevant items	Provisions	Sources used
	(4) Fiscal crimes, if the value of the subject of offence or reduction of public private amount due is in excess of the multiple of fifty minimum wages, defined on the basis of separate provisions, (5) illegal manufacture, possession or turnover in arms, ammunition, explosives, intoxicants, psychotropic substances and their precursors, as well as nuclear and radioactive materials, (6) defined in Article 8 of the Act of 6 June 1997 – Provisions implementing the Penal Code (Dz. U. No 88, item 554, as amended), (7) defined in Article 43-46 of the Act of 1 July 2005 on collection, storage and transplantation of cells, tissues and organs (Dz. U. No 169, item 1411), (8) prosecuted under international contracts and agreements".	
Does national law allow this tool to be used in cross border cases?	Some of the above activities include cross-border crimes by its nature but there is no certain specification on that matter.	
What thresholds must be passed for the use of this tool?	Life imprisonment (altoist this question does not apply directly here, as the Penal Code in Poland does not distinguish the crimes by availability of controlling methods that can be used in the investigative process).	
What types of stakeholder are involved in the implementation of this tool?	Police Commander in Chief, General Public Prosecutor, Voivodship Police Commander, the lower (Sejm) and upper (Senat) chamber of the Parliament. Their detailed roles, depending of the stage of the investigation and other circumstances are included in the below quotation from the Act on the Police: <u>Act on the Police:</u> Article 19. (..) 2. The provision referred to in Paragraph 1 shall be issued by the district court with territorial competence on account of the seat of the Police authority submitting the request. 3. In cases of the utmost urgency, where any delay could result in the loss of information or the obliteration or destruction of the evidence of a crime, the Police Commander in Chief or the Voivodship Police Commander may order, upon a written consent of the competent prosecutor referred to in Paragraph 1, operational control, submitting also a request for resolution in that matter to the district court with territorial competence. Should consent not be granted within 5 days from the day of ordering operational control, the managing authority shall withhold the operational control and perform destruction of materials collected during the control in the presence of a committee to be evidenced by a report. 4. The district court may permit the abandonment of destruction of materials referred to in Paragraph 3, on written request of the Police Commander in Chief or the Voivodship Police Commander, following a written consent of the competent prosecutor, if the materials are evidence or indicate intention to commit crime, which can be detected by way of operational control or preliminary investigation. 5. Should the need arise to order operational control in relation to a suspect or person charged, the request of the Police authority, referred to in Paragraph 1, to order operational control should be accompanied by information about the proceedings against that person. (..) 7. The request of the Police authority, referred to in Paragraph 1, to operational control ordered by the district court, should include in particular: (1) case number and cryptonym, if applicable, (2) description of the crime, stating, if possible, its legal qualification, (3) circumstances justifying the need to perform operational control, including stated or possible ineffectiveness or uselessness of other means, (4) personal data or other data facilitating unambiguous determination of the entity or object subject to operational control, stating the place or procedure for undertaking the control, (5) objective, time and type of operational control referred to in Paragraph 6. 8. Operational control shall be ordered for a period not exceeding 3 months. The District court may, upon written request of the Police Commander in Chief or the Voivodship Police Commander, following a written consent of the competent prosecutor, for a period not exceeding 3 subsequent months, issue a resolution on single extension of operational control, if the reasons for ordering the control have not been established. 9. In justified cases, when new circumstances important to prevent or detect crime or establish perpetrators and obtain evidence of crime appear, the district court may, upon a written request of the Police Commander in Chief, following a written consent of the General Public Prosecutor, issue a resolution on operational control for the period determined also after the periods referred to in Paragraph 8. 10. The provision of Paragraph 7 shall apply to requests referred to in Paragraphs 3, 4, 8 and 9 respectively. The court, prior to issuing the resolution referred to in Paragraphs 3, 4, 8 and 9, may wish to see the materials justifying the request, which were collected during operational control ordered for that case. 11. Requests referred to in Paragraphs 1, 3-5, 8 and 9 shall be examined by the district court	1. Act of 6 April 1990 on the Police, here and later referred as the Act on the Police (Ustawa z dnia 6 kwietnia 1990 r. o Policji). https://www.policja.pl/ftp/pliki/police_act.pdf

Relevant items	Provisions	Sources used
	individually, at the same time court proceedings relating to examination of the requests should be performed under conditions foreseen for submission, storage and provision of secret information and adequate application of the regulations issued pursuant to Article 181 § 2 of the Code of Criminal Procedure. The court sitting may be attended only by a prosecutor and a representative of the Police authority requesting the order of operational control. 12. Entities carrying out telecommunications activity and entities providing postal services shall ensure, at their own expense, technical and organisational conditions facilitating the operational control carried out by the Police. 13. Operational control should be completed immediately when the causes of its institution no longer exist, at the latest, however, upon the expiry date. 14. The Police authority referred to in Paragraph 1 shall notify the competent prosecutor about the results of operational control upon its completion, and upon his request also about the course of control. 15. Should evidence be obtained facilitating the institution of criminal proceedings or significant to the criminal proceedings in progress, the Police Commander in Chief or the Voivodship Police Commander shall provide the competent prosecutor with any and all materials collected during operational control, if necessary, with the request for institution of criminal proceedings. Provisions of Article 393 Paragraph 1 first sentence of the Code of Criminal Proceedings shall apply accordingly to proceedings before a court in respect to the materials. 16. The person subject to operational control shall not be provided with materials collected during the control. The provision is not in violation of the rights under Article 321 of the Code of Criminal Proceedings. 17. Materials collected during operational control, which do not include evidence facilitating the institution of criminal proceedings, shall be stored after the conclusion of control for the period of 2 months. They shall then be destroyed in the presence of a committee and the process evidenced in a report. The destruction of materials shall be ordered by the Police authority, which requested the operational control. 18. Procedures referred to in Paragraphs 1-11 shall not apply, if operational control is carried out following a written consent of the sender or recipient of information. 19. In cases referred to in Paragraph 18, operational control is ordered by the Police authority competent preliminary investigation of the case. 20. The ruling of the court concerning operational control referred to in Paragraphs 1, 3, 8 and 9, and the ruling concerning abandonment of destruction of materials collected during operational control referred to in Paragraph 4 may be appealed against by the Police authority, which requested such ruling. Provisions of the Code of Criminal Proceedings shall apply accordingly to the appeal. 21. The Minister competent for internal matters, upon consultation with the Minister of Justice and the Minister competent for communications, shall determine, by way of ordinance, mode of record of operational control and storage and submission of requests and orders, as well as storage, submission, processing and destruction of materials obtained during control, taking account of the necessity to ensure secret character of measures taken and materials obtained, and models of forms and registers used. 22. The General Public Prosecutor shall provide the lower (Sejm) and upper (Senat) chamber of the Parliament with information about the activity defined in Paragraphs 1-21, including information and data referred to in Article 20 (3).	
Which LEAs can use this tool?	+ Police + Border Control (<i>Straż Graniczna</i>) + Military Police (<i>Żandarmeria Wojskowa</i>) + Officers of the Revenue Intelligence unit of the Tax Office (<i>funkcjonariusze wywiadu skarbowego Urzędu Skarbowego</i>) + Special Services (<i>Służby Specjalne</i>): - Internal Security Agency / <i>Agencja Bezpieczeństwa Wewnętrznego (ABW)</i> - Central Anticorruption Bureau / <i>Centralne Biuro Antykorupcyjne (CBA)</i> - Military Counterintelligence Service / <i>Służba Kontrwywiadu Wojskowego (SKW)</i> - Military Intelligence Service / <i>Służba Wywiadu Wojskowego (SWW)</i>	
What are the rules to be followed for the implementation of this tool?	There is no separate section described as the "specific rules" in the Act on the Police, however some of the already mentioned paragraphs from the Article 19 (i.e. paragraph 9) could be interpreted as "specific rules", as well as there might be other internal regulations depending on the law enforcement body using this tool.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	There is no separate section described as the "specific restrictions" in the Act of the Police, however some of the already mentioned paragraphs from the Article 19 (i.e. paragraph 18) could be interpreted as such.	

Relevant items	Provisions	Sources used
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	The detailed process of granting the authorisation is described in the Act on the Police: <u>Act on the Police</u>: Article 19. (..) 2. The provision referred to in Paragraph 1 shall be issued by the district court with territorial competence on account of the seat of the Police authority submitting the request. 3. In cases of the utmost urgency, where any delay could result in the loss of information or the obliteration or destruction of the evidence of a crime, the Police Commander in Chief or the Voivodship Police Commander may order, upon a written consent of the competent prosecutor referred to in Paragraph 1, operational control, submitting also a request for resolution in that matter to the district court with territorial competence. Should consent not be granted within 5 days from the day of ordering operational control, the managing authority shall withhold the operational control and perform destruction of materials collected during the control in the presence of a committee to be evidenced by a report. 4. The district court may permit the abandonment of destruction of materials referred to in Paragraph 3, on written request of the Police Commander in Chief or the Voivodship Police Commander, following a written consent of the competent prosecutor, if the materials are evidence or indicate intention to commit crime, which can be detected by way of operational control or preliminary investigation. 5. Should the need arise to order operational control in relation to a suspect or person charged, the request of the Police authority, referred to in Paragraph 1, to order operational control should be accompanied by information about the proceedings against that person. (..) 7. The request of the Police authority, referred to in Paragraph 1, to operational control ordered by the district court, should include in particular: (1) case number and cryptonym, if applicable, (2) description of the crime, stating, if possible, its legal qualification, (3) circumstances justifying the need to perform operational control, including stated or possible ineffectiveness or uselessness of other means, (4) personal data or other data facilitating unambiguous determination of the entity or object subject to operational control, stating the place or procedure for undertaking the control, (5) objective, time and type of operational control referred to in Paragraph 6. 8. Operational control shall be ordered for a period not exceeding 3 months. The District court may, upon written request of the Police Commander in Chief or the Voivodship Police Commander, following a written consent of the competent prosecutor, for a period not exceeding 3 subsequent months, issue a resolution on single extension of operational control, if the reasons for ordering the control have not been established. 9. In justified cases, when new circumstances important to prevent or detect crime or establish perpetrators and obtain evidence of crime appear, the district court may, upon a written request of the Police Commander in Chief, following a written consent of the General Public Prosecutor, issue a resolution on operational control for the period determined also after the periods referred to in Paragraph 8. 10. The provision of Paragraph 7 shall apply to requests referred to in Paragraphs 3, 4, 8 and 9 respectively. The court, prior to issuing the resolution referred to in Paragraphs 3, 4, 8 and 9, may wish to see the materials justifying the request, which were collected during operational control ordered for that case. 11. Requests referred to in Paragraphs 1, 3-5, 8 and 9 shall be examined by the district court individually, at the same time court proceedings relating to examination of the requests should be performed under conditions foreseen for submission, storage and provision of secret information and adequate application of the regulations issued pursuant to Article 181 § 2 of the Code of Criminal Procedure. The court sitting may be attended only by a prosecutor and a representative of the Police authority requesting the order of operational control. 12. Entities carrying out telecommunications activity and entities providing postal services shall ensure, at their own expense, technical and organisational conditions facilitating the operational control carried out by the Police. 13. Operational control should be completed immediately when the causes of its institution no longer exist, at the latest, however, upon the expiry date. 14. The Police authority referred to in Paragraph 1 shall notify the competent prosecutor about the results of operational control upon its completion, and upon his request also about the course of control. 15. Should evidence be obtained facilitating the institution of criminal proceedings or significant to the criminal proceedings in progress, the Police Commander in Chief or the Voivodship Police Commander shall provide the competent prosecutor with any and all materials collected during operational control, if necessary, with the request for institution of criminal	1. Act of 6 April 1990 on the Police, here and later referred as the Act on the Police (Ustawa z dnia 6 kwietnia 1990 r. o Policji). https://www.policja.pl/ftp/pliki/police_act.pdf

Relevant items	Provisions	Sources used
	proceedings. Provisions of Article 393 Paragraph 1 first sentence of the Code of Criminal Proceedings shall apply accordingly to proceedings before a court in respect to the materials. 16. The person subject to operational control shall not be provided with materials collected during the control. The provision is not in violation of the rights under Article 321 of the Code of Criminal Proceedings. 17. Materials collected during operational control, which do not include evidence facilitating the institution of criminal proceedings, shall be stored after the conclusion of control for the period of 2 months. They shall then be destroyed in the presence of a committee and the process evidenced in a report. The destruction of materials shall be ordered by the Police authority, which requested the operational control. 18. Procedures referred to in Paragraphs 1-11 shall not apply, if operational control is carried out following a written consent of the sender or recipient of information. 19. In cases referred to in Paragraph 18, operational control is ordered by the Police authority competent preliminary investigation of the case. 20. The ruling of the court concerning operational control referred to in Paragraphs 1, 3, 8 and 9, and the ruling concerning abandonment of destruction of materials collected during operational control referred to in Paragraph 4 may be appealed against by the Police authority, which requested such ruling. Provisions of the Code of Criminal Proceedings shall apply accordingly to the appeal. 21. The Minister competent for internal matters, upon consultation with the Minister of Justice and the Minister competent for communications, shall determine, by way of ordinance, mode of record of operational control and storage and submission of requests and orders, as well as storage, submission, processing and destruction of materials obtained during control, taking account of the necessity to ensure secret character of measures taken and materials obtained, and models of forms and registers used. 22. The General Public Prosecutor shall provide the lower (Sejm) and upper (Senat) chamber of the Parliament with information about the activity defined in Paragraphs 1-21, including information and data referred to in Article 20 (3).	
What ongoing supervision is required for the use of this tool?	There is no "requirement" but according to the Act on the Police: <u>Act on the Police:</u> Article 19. 14. The Police authority referred to in Paragraph 1 shall notify the competent prosecutor about the results of operational control upon its completion, and upon his request also about the course of control.	1. Act of 6 April 1990 on the Police, here and later referred as the Act on the Police (Ustawa z dnia 6 kwietnia 1990 r. o Policji). https://www.policja.pl/ftp/pliki/police_act.pdf
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	Usage number of this investigative tool by authorised bodies during period included in available data is very low (i.e. 0 in 2013).	1. Use of the information gathered by operational means by the courts of the first instance (<i>Korzystanie w postępowaniu karnym przez sądy pierwszej instancji z informacji zebranych operacyjnie</i>), page 57 (available in Polish): https://iws.gov.pl/wp-content/uploads/2018/08/IWS_Szumi%C5%82o-Kulczycka-D._._.-z-inf.-zebranych-operacyjnie.pdf
Undercover / covert operations		
Relevant documents (legal and non-legal) that define the functioning of the tool	Regarding the police: 1. Act of 6 April 1990 on the Police, here and later referred as the <i>Act on the Police</i> (Ustawa z dnia 6 kwietnia 1990 r. o Policji).	1. Act of 6 April 1990 on the Police, here and later referred as the Act on the Police (Ustawa z dnia 6 kwietnia 1990 r. o Policji). https://www.policja.pl/ftp/pliki/police_act.pdf
How is the tool defined?	There is no legal definition of "Undercover / covert operation" (pol. <i>Operacja specjalna</i> or "<i>pod przykryciem</i>") included in the above acts. The undercover operation in the meaning of usage of false ID by the law enforcement officers is included in the section titled "Camouflage" (Article 20a) of the Act on the Police: <u>Article 20a. [Camouflage]</u> 1. On account of carrying out the tasks referred to in Article 1 (2) the Police shall ensure protection for the forms and methods of task performance, information, its own facilities and the particulars of police officers. 2. In the course of preliminary investigation, police officers may use documents which prevent determination of their particulars and the measures applied when performing official duties. 3. In special cases, Paragraph 2 may apply to persons referred to in Article 22 (1). 3a. A person shall not be guilty of a crime, if they:	

Relevant items	Provisions	Sources used
	(1) order the documents referred to in Paragraphs 2 and 3 to be drawn up or oversee drawing up of such documents, (2) draw up the documents referred to in Paragraphs 2 and 3, (3) assist in drawing up of the documents referred to in Paragraphs 2 and 3, (4) are a police officer or the person referred to in Paragraph 3 if they use the documents referred to in Paragraphs 2 and 3 for the purposes of preliminary investigation. 3b. Government administration authorities and local government authorities shall, within the scope of their competence, assist the Police in issuing and securing the documents referred to in Paragraphs 2 and 3. 4. The Minister competent for internal affairs shall, by way of ordinance, lay down detailed rules and procedure for issuance, use and storage of the documents referred to in Paragraphs 2 and 3, with due regard given to the types of documents and the purpose for which they are disclosed, the authorities and persons authorised to issue, use and store the documents, the period for which they are made available, measures ensuring protection of the documents, and the rules for storing and recording these documents.	
For what types of crime can the tool be used?	This tool does not depend on the type of crime.	1. Act of 6 April 1990 on the Police, here and later referred as the Act on the Police (Ustawa z dnia 6 kwietnia 1990 r. o Policji). https://www.policja.pl/ftp/pliki/police_act.pdf
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	Minister of the Internal Affairs as described in the Article 20a quoted above.	
Which LEAs can use this tool?	Police	
What are the rules to be followed for the implementation of this tool?	No detailed rules regarding that matter (other that indicated in article 20a of the Act on the Police quoted above)	1. https://www.policja.pl/ftp/pliki/police_act.pdf 2. https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-REF(2016)036-e
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	No detailed rules regarding that matter (other that indicated in article 20a of the Act on the Police quoted above)	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	Regarding the police: 1. Act of 6 April 1990 on the Police, here and later referred as the <i>Act on the Police</i> (Ustawa z dnia 6 kwietnia 1990 r. o Policji).	1. Act of 6 April 1990 on the Police, here and later referred as the Act on the Police (Ustawa z dnia 6 kwietnia 1990 r. o Policji). https://www.policja.pl/ftp/pliki/police_act.pdf
Specific range of application of the tool	<u>Act on the Police (1):</u> Article 22. 1. While performing its tasks, the Police may be assisted by persons who are not police officers. It shall be prohibited to disclose the particulars of persons who assist the Police in preliminary investigation activities. 1a. The particulars of persons referred to in Paragraph 1 may be disclosed only in cases and in accordance with the procedure laid down in Article 9 of the Act referred to in Article 20b.	1. Act of 6 April 1990 on the Police, here and later referred as the Act on the Police (Ustawa z dnia 6 kwietnia 1990 r. o Policji). https://www.policja.pl/ftp/pliki/police_act.pdf

Relevant items	Provisions	Sources used
	1b. The particulars of persons referred to in Paragraph 1 may be disclosed at the request of the prosecutor in the case of justified suspicion that a crime prosecuted on indictment has been committed in relation to performance of preliminary investigation activities. The particulars shall be disclosed in accordance with the procedure laid down in Article 9 of the Act referred to in Article 20b. 2. Persons who are not police officers may be remunerated for the assistance referred to in Paragraph 1. 2a. The costs of Police preliminary investigation in respect of which it is not possible to apply the regulations on public finances and accounting due to safety considerations referred to in Article 20a (1)-(3), as well as remuneration of persons referred to in Paragraph 1, shall be covered from a special operational fund. 3. The Minister competent for internal affairs shall determine, by way of ordinance, the rules for establishment and management of the operational fund. 4. In case of death of the persons referred to in Paragraph 1, injury to their health, or damage of their property as a result of or in the course of helping the Police, compensation shall be granted according to the rules and procedure laid down in ordinance of the Minister competent for internal affairs.	
How is the tool defined?	<u>Act on the Police (1):</u> Article 22. 1. While performing its tasks, the Police may be assisted by persons who are not police officers. It shall be prohibited to disclose the particulars of persons who assist the Police in preliminary investigation activities.	
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	Police	
What are the rules to be followed for the implementation of this tool?	No detailed rules regarding that matter (other that indicated in article 22 of the Act on the Police quoted above)	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	

Source: Author’s own elaboration

Portugal

Table 42 – Overview of national rules on investigative tools - Portugal

Relevant items	Provisions	Sources used
Controlled Delivery		

Relevant items	Provisions	Sources used
Relevant documents (legal and non-legal) that define the functioning of the tool	Law 144/99, of 31 August 1999 (international cooperation in criminal matters)	The Assembly of the Republic decrees, under the terms of paragraph c) of article 161 of the Constitution, to apply as a general law of the Republic,
How is the tool defined?	No specific definition is given in the law. The overall explanation is given. Like - It may be authorised on a case-by-case basis by the Public Prosecutor's Office, at the request of one or more foreign States	Art. 160 A (1)
For what types of crime can the tool be used?	No specific crimes are mentioned in the law. It only says «in the scope of cross-border criminal investigations related to offenses that admit extradition»	Art. 160 A (1) , Art. 160 A (2), Art. 160 A (3) a)
Does national law allow this tool to be used in cross border cases?	Yes. In fact this tool is widely used in only cross-border cases	Art. 160 A (1)
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	LEAs	Art. 160 A (9)
Which LEAs can use this tool?	Judicial Police is the ONLY implementing agency. No matter whichever department receives the request for controlled delivery, they have to pass the request to judicial police to execute it. Judicial police can take help of local police, if required.	Art. 160 A (8)
What are the rules to be followed for the implementation of this tool?	the following procedure has to follow. 1 - The request made to Portugal is submitted, through the Central Authority, for the appreciation of the Minister of Justice. 2 - The Minister of Justice may request information from the competent services to monitor the measures imposed in the sentence. 3 - If the Minister of Justice accepts the request, the Attorney General's Office shall forward it to the Public Prosecutor's Office at the Court of Appeal in the area of residence of the person concerned, for a judicial decision on its admissibility.	Art. 131 (1), (2), (3)
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	The controlled delivery can be granted for the following when: a) It is ensured by the competent foreign authorities that its legislation provides for criminal sanctions against the agents and that criminal action will be taken; b) The safety of the substances or goods in question is guaranteed by the competent foreign authorities against risks of escape or loss; and c) The competent foreign authorities undertake to communicate, as a matter of urgency, detailed information on the results of the operation and the details of the action taken by each of the offending agents, especially those who acted in Portugal.	Art. 160 A (3), a,b,c
What authorisation is needed for the use of this tool?	N/A	
What ongoing supervision is required for the use of this tool?	The magistrate of the Public Prosecutor in the district of Lisbon is competent to decide on the request for controlled deliveries	Art. 160 A (9)
Is there any national case law relating to the use of this tool in cross-border crime cases?	There is no specific ongoing supervision is required because mainly controlled deliveries are planned.	Art. 160 A (4)
Data available on the number of times this tool has been used for SOC cases	N/A	
Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	N/A	
How is the tool defined?	N/A	
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	

Relevant items	Provisions	Sources used
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	Law no. 93/99 (witness protection law)	Act n.º 93/99, of 14 July 1999: Governing the enforcement of measures on the protection of witnesses in criminal proceedings. This Act shall enter into force on the 60th day following its publication.
How is the tool defined?	Witness means any person who, notwithstanding his status towards the procedural law, is in possession of any information or knowledge necessary to the disclosure, apprehension or evaluation of facts subject to investigation and which are likely to represent a danger to that person.	Chapter 1, section 2, a)
For what types of crime can the tool be used?	Not mention of any crimes is given in the law. Whereas it says - The testimony or the statement relates to criminal offences stated in human trafficking (section 169), any organised crime (art. 299) (did not specified anything further in penal code), Terrorism (art. 300) of the Criminal Code or to criminal offences committed by whoever belongs to a criminal association, in the scope of its purpose or activity, and to which corresponds an imprisonment sentence equal or superior to eight years;	CHAPTER III Restriction regarding the disclosure of the witness's identification features, Section 16 (a) Art. 300 (1) penal code link https://dre.pt/web/guest/legislacao-consolidada/-/lc/141459984/202008310400/73871627/diploma/indice
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	Witness in criminal offences stated in sections 169, 299, 300 or 301 of the Criminal Code are obliged to have prison of 8 or higher years.	CHAPTER III Restriction regarding the disclosure of the witness's identification features, Section 16 (a)
What types of stakeholder are involved in the implementation of this tool?	Judiciary Police – Polícia Judiciária (PJ) -The PJ is the national police force and has the exclusive legal attribution for criminal investigations related to the 'criminal association' offence and for the investigation related to a catalogue of other serious offences, particularly when said offences have a cross-border dimension or are committed in a 'highly organised' form. This is a highly specialised body comprising: the National Unit for Economic and Financial Crime; the National Unit for Counterterrorism; the National Unit for Drug Trafficking. Being the main law enforcement agency in the country, the PJ hosts liaison officers from other national forces, as well as from Europol and Interpol. At the National Level, there are formal cooperation institutions, like the Coordinator Council for Criminal Investigation, where members of different police forces have a seat; and more pragmatic and case-by-case opportunities, like the possibility to set up a national joint investigation teams for special cases. Central Department for Investigation and Prosecution – Department of Central de Investigação e Ação Penal (DCIAP) - The DCIAP is a national department of Public Prosecution. It coordinates and oversees preventive actions and investigations conducted by police forces (mainly PJ) with a legal attribution for the prosecution of 'violent, especially complex or highly organised crime' - It coordinates the investigations made by different police forces. It coordinates also the work of other prosecution departments operating at the regional level. In this last instance it not only shares information, but also advocates concrete investigations when a connection to organised crime arises.	Page 567 of AMOC report of EU. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/20150312_1_amoc_report_020315_0_220_part_2_en.pdf
Which LEAs can use this tool?	Judiciary Police is the important to execute the activities along with Central Department for investigation and prosecution (DPCIAP)	Art. 160 A (8) of international cooperation law
What are the rules to be followed for the implementation of this tool?	The court may decide to permit the use of this tool upon the request of the Public Prosecutor	Chapter 2, section 4, 1)
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Non-disclosure (which is the right to non-disclosure for the safety of lives or protection of properties etc.) is granted to witness to prevent basic human right as it may be threat to his/her life or his/her relatives or property. Besides this, special programme of security is allowed under which following is stated - Any witness, the respective wife or husband, ancestors, descendants, brothers and sisters or any other persons in close contact with him, may benefit from a special programme of security during the running of the proceeding or even after its closure, provided the following concurrent conditions occur - a) The testimony or statement concern the criminal offences laid down in article 16 of witness protection law. b) There is a serious danger to their lives, physical or psychical integrity or freedom;	Section 13; section 21 (1), (2), (3)

Relevant items	Provisions	Sources used
	c) The testimony or the statement constitutes a contribution which is deemed, or has proved to be, essential to the ascertainment of the truth. to induce the witness to the indirect disclosure of his identity.	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Ministry of justice (judge) can grant to use this tool upon requesting of public prosecutor. Also examining judge can give the order and also to provide the special programme safety of witness.	Section 13; section 21 (1), (2), (3)
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Surveillance		
Relevant documents (legal and non-legal) that define the functioning of the tool	Law No. 37/2008	- Publication: Diário da República no. 151/2008, Series I of 2008-08-06. Issuer: Assembly of the Republic. Diploma Type: Law. Number: 37/2008. Pages: 5281 - 5289. ELI: https://data.dre.pt/eli/lei/37/2008/08/06/p/dre/pt/html. Implementation: 2008-09-05, under the terms of art. 59th. Diário da República no. 151/2008, Series I of 2008-08-06
Specific range of application of the tool	Surveillance can be done of Places or person. Recording of voice and image is also possible, in serious organised crime investigations. Tracking of the position of cellular devices.	art 4 (2) art. 6 of Law n. 5/2002, of 11 January 2002 (with special judicial permission) art. 252-A of Penal Procedure Code (with judicial permission, in case of danger to life or personal safety of someone).
How is the tool defined?	Judiciary police (PJ) can have access to the information necessary for the characterisation, identification and location of situations, being able to proceed with the identification of people and carry out surveillance, if necessary, using all means and sound and image registration techniques, as well as magazines and searches, under the terms of the Criminal Procedure Code and complementary legislation.	Art 4 (3)
For what types of crime can the tool be used?	in national law NO specific crime is mentioned whereas simply «crime» word is used.	- International cooperation law 144 --- Art. 160 A (1) , Art. 160 A (2), Art. 160 A (3) a) Art. - art. 145, n. 5 and n. 9, of Law n. 144/99, of 31 August 1999
Does national law allow this tool to be used in cross border cases?	Yes. Cross-border surveillance is not stated autonomously, but it is possible, in terms of practical police cooperation, to receive elements of foreign police authorities engaged, with national elements, in surveillance operations or for other investigative purposes. With authorisation of the minister of Justice, that can delegate that authorisation in the national director of the PJ, if not requested under an international treaty or EU law	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	The following officers/positions of judiciary police can act: a) National director; b) Deputy national directors; c) Directors of national units; d) Directors of territorial units; e) Subdirectors of territorial units; f) Criminal investigation advisers; g) Senior criminal investigation coordinators; h) Criminal investigation coordinators; i) Chief inspectors and legal entities like Central Department for Investigation and Prosecution	Chapter 2, Art.11 (1) a to I
Which LEAs can use this tool?	Judiciary police and prosecution	Art. 160 A (8) of international cooperation law
What are the rules to be followed for the implementation of this tool?	in this law, specific procedure is not mention but following from the other laws we can infer that judiciary police can request to public procedure for conduct the surveillance.	Chapter 2, section 4, 1)
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	National director of Judiciary police has the right to execute the surveillance in cooperation with LEAs.	Art. 12 (3)
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime	N/A	

Relevant items	Provisions	Sources used
cases? If yes can you please indicate the relevant statistics?		
Undercover / covert operations		
Relevant documents (legal and non-legal) that define the functioning of the tool	Law n. 101/2001, of 25 August 2001	The Assembly of the Republic decrees, under the terms of paragraph c) of article 161 of the Constitution, to apply as a general law of the Republic.
How is the tool defined?	Undercover actions are considered to be those carried out by criminal investigation officials or by a third party acting under the control of the Judiciary Police to prevent or prosecute the crimes indicated in this law, with their quality and identity concealed	Art. 1 (1)
For what types of crime can the tool be used?	a) Voluntary homicide, as long as the agent is not known; b) Against freedom and against sexual self-determination to which, in the abstract, a penalty of more than 5 years in prison corresponds, provided that the agent is not known, or whenever they are expressly referred to offended children under 16 or other incapacitated; c) Relating to the traffic and addiction of stolen or stolen vehicles; d) Slavery, kidnapping and kidnapping or taking hostages; e) Trafficking in persons; f) Terrorist organisations, terrorism, international terrorism and terrorist financing; g) Capture or attack on the security of transport by air, water, railroad or highway to which, in the abstract, corresponds to a sentence equal to or greater than 8 years in prison; h) Executed with bombs, grenades, explosive materials or devices, firearms and trapped objects, nuclear, chemical or radioactive weapons; i) Theft from credit institutions, public finance offices and post offices; j) Criminal associations; l) Relating to trafficking in narcotic drugs and psychotropic substances; m) Money laundering, other goods or products; n) Corruption, embezzlement and economic participation in business and influence peddling; o) Fraud in obtaining or diverting a subsidy or subsidy; p) Economic and financial offenses committed in an organised manner or using computer technology; q) Economic and financial offenses with an international or transnational dimension; r) Counterfeiting of currency, credit titles, sealed values, stamps and other similar values or the respective transfer; s) Relating to the securities market.	Art 2 (a to s)
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	It is not punishable the conduct of the covert agent who, in the context of a covert action, consubstantiates the practice of preparatory acts or execution of an infraction in any form of co-participation other than the instigation and mediated authorship, whenever it keeps the due proportionality for the purpose of it.	Art 6 (1)
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	Judiciary police and LEAs	- Art. 160 A (8) of international cooperation law - Art 3 (1 to 6)
What are the rules to be followed for the implementation of this tool?	1 - The covert actions must be suitable for the purposes of criminal prevention and repression identified in concrete, namely the discovery of evidential material, and proportional both to those purposes and to the seriousness of the crime under investigation. 2 - No one can be forced to participate in covert action. 3 - The performance of a covert action within the scope of the investigation depends on the prior authorisation of the competent Public Prosecutor, being mandatorily communicated to the investigating judge and considering it validated if no refusal order is issued within the next seventy-two hours. . 4 - If the action referred to in the preceding paragraph takes place within the scope of criminal prevention, the criminal investigating judge is competent for authorisation, following a proposal by the Public Ministry. 5 - In the cases referred to in the preceding paragraph, the competence for the initiative and the decision is, respectively, the magistrate of the Public Prosecution at the Central Department of Investigation and Criminal Action and the judge of the Central Court of Criminal Instruction. 6 - The Judiciary Police will report the intervention of the covert agent to the competent judicial authority within a maximum period of forty-eight hours after the end of that period	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	1 - Criminal police officers may act under a fictitious identity. 2 - The fictitious identity is assigned by order of the Minister of Justice, following a proposal by the national director of the Judiciary Police. 3 - The identity referred to in the preceding paragraph is valid for a period of six months, which may be extended for periods of the same duration, with the criminal investigation official to whom	Art 5 (1,2,3,4,5)

Relevant items	Provisions	Sources used
	it is attributed authorised to, during that period, act under the fictitious identity, either in exercise of concrete investigation either generically in all circumstances of legal and social trafficking. 4 - The order that assigns the fictitious identity is classified as secret and must include a reference to the real identity of the covert agent. 5 - The Judiciary Police is responsible for managing and promoting the updating of the fictitious identities granted under the terms of the previous numbers.	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	The performance of a covert action within the scope of criminal investigating judge is competent for authorisation, following a proposal by the Public Ministry.	Art 3 (4)
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	Penal Procedure code	Decree-Law No. 48/95. Diário da República no. 63/1995, Series IA of 1995-03-15. Number: 48/9. Issuing. Entity (s): Justice ministry. Source: DIARIO DA REPUBLICA - 1st SERIE A, Nº 63, from 1995-03-15, Page 1350 - 1416. Implementation: The revised Penal Code and the present decree-law come into force on 01.10.1995 https://data.dre.pt/eli/dec-lei/48/1995/p/cons/20200831/en/html
Specific range of application of the tool	1) The use of informants is not prohibited by Portuguese law, since law enforcement has a general right to obtain information for crime prevention and investigation. An "informants regime" is not autonomously established by law. 2) the absence of punishment if the agent cooperates in the same terms with the authorities, namely regarding collection of evidence, the identity of other perpetrators or the dismantle of a criminal association	1) the previous study finds the same results, 2) art 31 of Law n. 15/93, of 15 January 1993
How is the tool defined?	N/A	
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	

Source: Author's own elaboration

Romania

Table 43 – Overview of national rules on investigative tools - Romania

Relevant items	Provisions	Sources used
Controlled Delivery		
Relevant documents (legal and non-legal) that define the functioning of the tool	Article 138 (1) i), art. 151 Criminal Procedure Code (both regulated by law 135/2010)	Article 138 (1) i), art. 151 Criminal Procedure Code (both regulated by law 135/2010)
How is the tool defined?	Controlled delivery designates a surveillance and investigation technique allowing for the entry, transit or exit from the territory of the country of illicit or suspect consignments of narcotic drugs, psychotropic substances or substances substituted for them as well as other goods, considered to be subject of smuggling, with the knowledge and under the supervision of their competent authorities, with a view to the investigation of an offence and the identification the persons involved in the committing of the offence.	Article 138 (1) i), Article 138 (12), Article 151 Criminal Procedure Code (Law 135/2010)
For what types of crime can the tool be used?	Illicit drugs trade, trafficking of firearms, trafficking of stolen goods, trafficking of explosive or nuclear materials, radioactive materials, money amounts and other proceeds resulting from illegal activities or of items used for the purpose of perpetrating offenses	Article 151 (2) a) Criminal Procedure Code (Law 135/2010)
Does national law allow this tool to be used in cross border cases?	Law 302/2004 for allows the use of this tool in cross-border cases (Article 237). The competent Romanian judicial authorities authorize, upon request, under the conditions provided by Romanian law, controlled deliveries, within criminal proceedings regarding offenses that may give rise to extradition. The controlled deliveries are carried out according to the Romanian law. The provisions of this Article shall also apply accordingly if assistance is requested by the Romanian judicial authorities.	Article 237, Law 302/2004 regarding the judicial international cooperation
What thresholds must be passed for the use of this tool?	The tool can be used for the list of offences described above, or for any offence that states a term of imprisonment of 7 years or more.	Article 151 (2) a) Criminal Procedure Code (Law 135/2010)
What types of stakeholder are involved in the implementation of this tool?	The actors involved in the implementation of the tool are the prosecutor that oversees the criminal investigation (authorisation role) and the undercover investigators (execution role), in collaboration with law enforcement bodies.	Article 151 (6) Criminal Procedure Code (Law 135/2010)
Which LEAs can use this tool?	The LEAs allowed to use this tool are: 1. Criminal specialised investigation bodies (joint team police - prosecutors): - the Directorate for Investigations of Organised Crime and Terrorism (DIICOT), - - the National Anticorruption Directorate (DNA), 2. Directorate for Combatting Organised Crime- General Inspectorate of the Romanian Police (DCCO) 3. Economic Crimes Investigation Directorate (DICE)	1. OUG 78/2016, approved by law 120/2018, http://legislatie.just.ro/Public/DetaliuDocument/183842 2. OUG 43/2002, http://legislatie.just.ro/Public/DetaliuDocument/35165 3. Law 39/2003, modified by law 255/2013; http://www.cdep.ro/pls/legis/legis_pck.htm_act_text?id=39932 4. https://www.politiaromana.ro/ro/politia-romana/unitati-centrale/directia-de-combatere-a-criminalitatii-organizate 4. https://www.politiaromana.ro/ro/politia-romana/unitati-centrale/directia-de-investigare-a-criminalitatii-economice
What are the rules to be followed for the implementation of this tool?	A controlled delivery may be authorised only in the following situations: a) if persons involved in illegal transport of drugs, weapons, stolen items, explosive or nuclear materials, radioactive materials, money amounts and other proceeds resulting from illegal activities or of items used for the purpose of perpetrating offenses could not be discovered or arrested in other ways or if this implies extreme difficulties that would harm the investigation or would be a threat against the safety of persons or of high value goods; b) if the discovery or proving of offenses committed in relation to the delivery of illegal or suspicious transports is impossible or extremely difficult in other way. In case of transnational activities, a controlled delivery can be performed under the terms established by the prosecutor supervising or conducting the criminal investigation who orders such measure, and makes sure that the transited states' authorities: a) agree with the entry of the illegal or suspicious transport on their territory and with its exit from their territory; b) guarantee that the illegal or suspicious transport is permanently monitored by the competent authorities; c) guarantee that a prosecutor, law enforcement body or other competent state authorities are informed of the results of the criminal investigation against persons accused of the offense subject to this special investigation method. Article 237 from law 302/2004 (regarding the judicial international cooperation), which regulates the international judicial cooperation in criminal matters, specifies that: The competent Romanian judicial authorities authorize, on request, in the conditions stipulated by the Romanian law, controlled deliveries, as part of criminal procedures regarding offences that may allow extradition. In addition, these stipulations also apply in case the assistance is requested by the Romanian judicial authorities.	Article 151 (1), (2), (3) Criminal Procedure Code (Law 135/2010), Article 237 from Law 302/2004 regarding the judicial international cooperation
Safeguards provided by national criminal laws to protect the rights of the	There are no specific safeguards in place, but the rules that need to be followed for implementation display a level of strictness that discourages abuse.	

Relevant items	Provisions	Sources used
individuals, ensure proportionality, and protect rule of law (if any)		
What authorisation is needed for the use of this tool?	A controlled delivery may be authorised by the prosecutor supervising or conducting the criminal investigation, through a prosecutorial order, upon request by institutions or bodies of competent jurisdiction. A prosecutorial order is a procedural act/document, in which the Prosecutor or the criminal investigation body records a provision regarding criminal investigation/prosecution acts or measures. According to Article 286 (2), every prosecutorial order has to contain a basic list of elements: 1) The name of the Prosecutor's Office and issue date 2) Name and capacity of the issuer 3) The offence covered by the investigation, its legal classification, and, where appropriate, data regarding the suspect or the defendant 4) The object of the act or measure, as well as the underlying reasons of fact or law 5) Where appropriate, indication of available appeal and the term in which it can be exercised 6) Data regarding precautionary measures, safety measures of medical nature and preventive measures taken during the investigation 7) Other elements prescribed by the law (each tool prescribes if the order requires elements in addition to those prescribed in the general norm) 8) Signature of the issuer By 'institutions or bodies of competent jurisdiction', it is meant: criminal investigation bodies (law enforcement and judiciary) if the request originates from Romania; if the request originates from a different country, it may differ according to the legislation of that country.	Article 151 (1) Criminal Procedure Code (Law 135/2010)
What ongoing supervision is required for the use of this tool?	The supervision for the use of this tool is ensured by the prosecutor who oversees the criminal investigation, in coordination with: a) authorities that, according to law, have to verify and supervise the entry, transit or exist of the goods from the territory (if the controlled delivery takes place in Romania) b) the competent authorities of the transited country (if the controlled delivery involves cross-border activities) There are no additional regulated requirements which the prosecutor must adhere to, in monitoring the use of controlled delivery.	Article 151 (1), (2) b), (3) b), (6) Criminal Procedure Code (Law 135/2010)
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Data available on the number of times this tool has been used for SOC cases	N/A	
Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	Not as such as Romania is not a Schengen state, but the foreign agents may act on the territory of Romania on the basis of article 239, law 302/2004 regarding the judicial international cooperation. Article 239 (Law 302/2004) regulates joint investigation teams. Joint investigation teams can be established and can function on the territory of Romania and of other states, with a view to facilitate criminal investigations. The procedures that regulate the functioning of such teams, as well as competence, duration, location, setup, capacities, scope and the conditions in which the members can take part in investigation activities are settled in a written agreement. The national EUROJUST member or his deputy may participate in the activities of the joint investigation team. In relation with EU Member States or Member States part of the Convention from 19 June 1990 for the implementation of the Schengen Agreement from 14 June 1985 regarding the gradual elimination of controls on common borders, the written agreement is concluded by the Chief Prosecutor of the public prosecutor's office in which the prosecutor carrying out or supervising the criminal investigation operates or, where there is no ongoing criminal proceedings on the territory of Romania, irrespective of the nature of the offence, by the General Prosecutor of the Public Prosecutor's Office of the High Court of Cassation and Justice or by the prosecutor appointed by him. In relation to non-Eu Member States, the agreement shall be concluded by the Prosecutor General of the Public Prosecutor's Office of the High Court of Cassation and Justice or by the Prosecutor appointed by him. In order to set up joint investigation teams, in the case of offences which, according to the law, are given to the Directorate for the Investigation of Organised Crime and Terrorism or the National Anti-Corruption Directorate, the agreement shall be concluded by their chief prosecutors or by the prosecutor appointed by them. A joint investigation team may be created especially in the following cases: (a) in the context of an ongoing procedure in the requesting State, difficult investigations involving significant human and other means concerning both States are required;	Article 239, Article 240 Law 302/2004 regarding the judicial international cooperation

Relevant items	Provisions	Sources used
	(b) several States carry out investigations requiring coordinated and concerted action in the States concerned. The request for the formation of a joint investigation team may be made by any State concerned. The team shall be formed in one of the States where the investigation is to be carried out. The request for the formation of a joint investigation team shall include proposals relating to the composition of the team. The members of the joint team appointed by the Romanian authorities shall be members, while those appointed by a foreign State shall be seconded members. The work of the joint investigation team in the territory of the Romanian State shall be carried out in accordance with the following general rules: a) the team leader is a representative of the competent Romanian judicial authority; b) the team's actions are carried out in accordance with Romanian law. Team members and seconded team members shall carry out their duties under the responsibility of the person referred to in (a). Members seconded to the Joint Investigation Team shall be entitled to be present at carrying out any procedural acts, unless the team leader decides otherwise. Where the work of the Joint Investigation Team is carried out in the territory of another State, if it is considered necessary to carry out investigation acts on the territory of Romania, the prosecutor who is a member of the joint investigation team may ask the Romanian authorities to carry out those acts, without the other participating States submitting an application for judicial cooperation, unless the arrest of a person is requested with a view to extradition or surrender, as the case may be. The procedures necessary to carry out the activity in Romania will be those applicable to criminal investigation activities, according to Romanian law. A member seconded to the Joint Investigation Team may, in accordance with his national law and within the limits of his powers, provide the team with information which is available to the State which seconded him for the purpose of carrying out the criminal investigations carried out by the team. Information normally obtained by a member or a seconded member in the context of participation in a joint investigation team and which cannot otherwise be obtained by the competent authorities of the States concerned may be used for the following purposes: a) for the purpose for which the team was created; b) to discover, investigate or prosecute other offences, with the consent of the State in whose territory the information was obtained; c) in order to prevent an imminent and serious danger to public security and in compliance with the provisions laid down in a).b); d) for other purposes, provided that this is agreed by the States which formed the team. In the case of joint investigation teams operating on the territory of Romania, seconded members of the team shall be treated as Romanian members in respect of the offences committed against them or by them. In addition, Article 240 (Law 302/2004 regarding the judicial international cooperation) regulates cross-border surveillance. Subject to the existence of contrary provisions in the Convention applicable in relation to that State, agents of a foreign State who, in the context of a judicial investigation, supervise in the territory of that State a person alleged to have participated in the commission of an offence giving rise to extradition or a person to whom there are serious grounds to believe that it may lead to the identification or location of the person mentioned above , are authorised to continue this supervision on the territory of the Romanian State on the basis of a request for legal aid submitted in advance. Upon request, supervision may be exercised by the competent Romanian authorities. The application for legal aid referred to above shall be addressed to the Public Prosecutor's Office of the High Court of Cassation and Justice and shall contain all relevant information in question, in accordance with the provisions of the applicable Convention. By authorisation the Prosecutor's Office of the High Court of Cassation and Justice will be able to lay down certain conditions. When, for reasons of urgency, the prior authorisation of the Romanian State cannot be requested, foreign agents acting in the criminal investigation are authorised to continue on the territory of Romania the supervision of a person suspected of having committed one of the acts listed below, under the following conditions: a) the border crossing will be communicated immediately, during surveillance, to the Prosecutor's Office of the High Court of Cassation and Justice, as well as to the border police structure set up within the border crossing point; (b) an application for legal aid shall be made in accordance with the general procedure. The reasons for crossing the border without prior authorisation shall be forwarded without delay. Surveillance may be carried out only under the following conditions: (a) surveillance agents must comply with the provisions of this Article and of Romanian law;	

Relevant items	Provisions	Sources used
	(b) subject to the exceptional circumstances referred to above, the agents shall carry with them a document attesting that they have been granted permission; (c) surveillance agents must be permanently able to justify their official status; (d) surveillance agents may carry their armaments during surveillance, unless, by authorisation, the Public Prosecutor's Office of the High Court of Cassation and Justice has provided otherwise; its use is prohibited, except in the case of self-defence; (e) entry into a person's home and other places inaccessible to the public is prohibited; (f) surveillance agents may neither detain nor arrest the supervised person; (g) any surveillance operation will be recorded in a report to the Public Prosecutor's Office of the High Court of Cassation and Justice, which shall also require the in-person presentation of the agents who carried out the surveillance; (h) the authority of the State to which the agents who carried out the surveillance belong, at the request of the competent Romanian authority, may assist in the subsequent investigation of the operation, including judicial proceedings; (i) the authorities of the State to which the surveillance agents belong, at the request of the Romanian authorities, shall contribute to the smooth conduct of the investigation following the operation in which they participated, including judicial proceedings. The surveillance conducted in conditions of urgency (detailed above) may take place only for one of the following facts: (a) first-degree murder and murder; (b) serious sexual offences, including rape and sexual abuse of minors; (c) destruction and first-degree destruction committed by arson, explosion or any such means; (d) counterfeiting and falsification of means of payment; (e) theft and robbery in aggravated form, as well as the receipt of stolen goods; (f) embezzlement; (g) unlawful deprivation of liberty; (h) offences of human trafficking, trafficking in minors, use of the services of an exploited person, child pornography; (i) offences relating to drug trafficking or precursors; (j) offences relating to non-compliance with the regime of weapons and ammunition, explosive materials, nuclear materials and other radioactive materials; (k) illegal transport of toxic and harmful waste; (l) migrant trafficking, facilitating illegal stay in Romania; (m) blackmail. This kind of supervision shall cease if the authorisation has not been obtained within 5 hours of crossing the State border and at the request of the Public Prosecutor's Office of the High Court of Cassation and Justice.	
How is the tool defined?	N/A	
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime	N/A	

Relevant items	Provisions	Sources used
cases? If yes can you please indicate the relevant statistics?		
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	Section 5: Article 125, 126, 127, 128, 129, 130 Criminal Procedure Code (regulated by Law 135/2010)	Section 5: Article 125, 126, 127, 128, 129, 130 Criminal Procedure Code (regulated by Law 135/2010)
How is the tool defined?	The tool regulated by Section 5 entails two components: 1. Protection of threatened witnesses: If there is a reasonable suspicion that the life, physical integrity, freedom, assets or professional activity of a witness or of a member of their family could be jeopardised as a result of the data provided by them to judicial bodies or of their statements, the judicial bodies of competent jurisdiction shall grant them the status of threatened witness and shall order one or more of the protection measures set by Arts. 126 or 127, (will be detailed below) as applicable. 2. Protection of vulnerable witnesses The prosecutor or, as applicable, the court may decide to grant the status of vulnerable witness to the following categories of persons: a) witnesses who suffered a trauma as a result of the committed offense or of the subsequent behaviour of a suspect or defendant; b) underage witnesses. At the moment of granting the status of vulnerable witness, the prosecutor and the court may order protection measures set by Art. 126 par. (1) items b) and d) or, as applicable, by Art. 127 items b) - e), which apply accordingly. Distortion of the voice and image is not mandatory.	Article 125, Article 130 Criminal Procedure Code (regulated by Law 135/2010)
For what types of crime can the tool be used?	The information available does not supply an answer.	
Does national law allow this tool to be used in cross border cases?	Article 253 (Law 302/2004) allows the use of this tool in cross-border cases.	Article 253, Law 302/2004 regarding the judicial international cooperation
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	The actors involved in the implementation of the tool are the following: 1. In the criminal investigation phase: a) the witness, one of the parties to the proceedings or one of the procedural subjects (requesting) b) prosecutor (authorizes; can also decide ex officio) 2. in the criminal trial phase: a) prosecutor, the witness, one of the parties to the proceedings or one of the procedural subjects (requesting) b) the court (judiciary) authorizes, but can also decide ex officio	Article 125, 126, 127, 128, 129, 130 Criminal Procedure Code (regulated by Law 135/2010)
Which LEAs can use this tool?	The LEAs allowed to use this tool are: 1. Criminal specialised investigation bodies (joint team police - prosecutors): - the Directorate for Investigations of Organised Crime and Terrorism (DIICOT), - - the National Anticorruption Directorate (DNA), 2. Directorate for Combatting Organised Crime- General Inspectorate of the Romanian Police (DCCO) 3. Economic Crimes Investigation Directorate (DICE)	1. OUG 78/2016, approved by law 120/2018, http://legislatie.just.ro/Public/DetaliuDocument/183842 2. OUG 43/2002, http://legislatie.just.ro/Public/DetaliuDocument/35165 3. Law 39/2003, modified by law 255/2013; http://www.cdep.ro/pls/legis/legis_pck.http_act_text?id=39932 4. https://www.politiaromana.ro/ro/politia-romana/unitati-centrale/directia-de-combatere-a-criminalitatii-organizate 4. https://www.politiaromana.ro/ro/politia-romana/unitati-centrale/directia-de-investigare-a-criminalitatii-economice
What are the rules to be followed for the implementation of this tool?	1. Protection measures ordered during the criminal investigation During the criminal investigation, once that the status of threatened witness was granted, the prosecutor shall order the application of one or more of the following measures: a) surveillance and guard of the witness' residence or providing of a temporary dwelling space; b) accompanying and ensuring protection to the witness or to their family members during travels; c) protection of identity data, by issuing them a pseudonym under which the witness shall sign their statement; d) hearing of a witness without them being physically present, through audio-video transmission devices, with their voice and image distorted, when the other measures are not sufficient. The prosecutor orders the application of protection measures ex officio or upon request by the witness, one of the parties or a main trial subject. The prosecutor orders the granting of the status of threatened witness and the application of protection measures through a reasoned order, which is stored under confidentiality terms. The prosecutor checks, at reasonable time intervals, whether the conditions having imposed the taking of protection measures continue to exist, and if not, they shall order, through a reasoned order, their termination. 2. Ordering a witness protection measure during the trial	Article 126, Article 128 Criminal Procedure Code (Law 135/2010)

Relevant items	Provisions	Sources used
	The court orders the application of protection measures ex officio, upon request by the prosecutor, the witnesses, the parties or the victim. A proposal filed by the prosecutor includes: a) name of the witnesses to be heard at the trial stage and in whose respect the ordering of a protection measure is sought; b) an actual reasoning of the danger seriousness and of such measure need. When such application is filed by the other persons listed, the court may order that the prosecutor conduct verifications, on an emergency basis, in respect of the soundness of such protection request. These rules also apply to the vulnerable witness status.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	) In case of application of the protection measures listed under par. (1) items c) and d)(protection of identity data, by issuing them a pseudonym under which the witness shall sign their statement; hearing of a witness without them being physically present, through audio-video transmission devices, with their voice and image distorted, when the other measures are not sufficient)., witness statements shall not include their real address or their identity data, these being recorded in a special register to which only criminal investigation bodies, the Judge for Rights and Liberties, the Preliminary Chamber Judge or the court have access, under confidentiality terms.	Article 126 (3) Criminal Procedure Law (Law 135/2010)
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	During the criminal investigation phase, the authorisation is provided by the prosecutor. During the criminal trial phase, the authorisation is provided by the judiciary body.	Article 126, Article 128 Criminal Procedure Code (Law 135/2010)
What ongoing supervision is required for the use of this tool?	The supervision for the use of this tool is ensured by the prosecutor who oversees the criminal investigation. The prosecutor checks, at reasonable time intervals, whether the conditions having imposed the taking of protection measures continue to exist, and if not, they shall order, through a reasoned order, their termination.	Article 126 (5) Criminal Procedure Code (Law 135/2010)
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Surveillance		
Relevant documents (legal and non-legal) that define the functioning of the tool	Article 138 (1) a) b) c) d) , Article 139 Criminal Procedure Code, (both regulated by law 135/2010)	Article 138 (1) a) b) c) d) , Article 139 Criminal Procedure Code, (both regulated by law 135/2010)
Specific range of application of the tool	The types of surveillance activities regulated by the national legislation are incorporated in the concept of electronic surveillance: - Audio surveillance (wiretapping of communications or of any type of remote communication) - Visual surveillance (video, audio or photo surveillance) - Tracking surveillance (tracking or tracing with the use of technical devices) - Data surveillance (accessing a computer system) All of the types of surveillance activities are regulated under the title of 'electronic surveillance' and they follow the general procedure described in articles 139, 140, 141, 142, 143, 144, 145, 146 from the Criminal Procedure Code. Nevertheless, the request forwarded to the Judge for Rights and Liberties must specify for which particular surveillance activity the authorisation is sought.	Article 138 (1) a) b) c) d) , 139, 140, 141, 142, 143, 144, 145, 146 Criminal Procedure Code, (all regulated by law 135/2010)
How is the tool defined?	Wiretapping of communications or of any type of messages designates the Wiretapping, accessing, monitoring, collection or recording of communications via phone, computer system or any other communication device. Accessing a computer system designates the penetration of a computer system or of other data storage device either directly or from a distance, through specialised programs or through a network, for the purpose of identifying evidence. Video, audio or photo surveillance is the taking of pictures of persons, the observation or recording of their conversations, gestures or other activities. Tracking or tracing with the use of technical devices is the use of devices that establish the location of the person or the object to which such devices are attached.	Article 138 (1) a) b) c) d) , Article 139 Criminal Procedure Code, (both regulated by law 135/2010)
For what types of crime can the tool be used?	Electronic surveillance may be ordered in case of offenses against national security stipulated by the Criminal Code and by special laws (offences against national security stipulated by the Criminal Code and by special laws: a. Treason - Article 394 Criminal Code	Article 139 (2) Criminal Procedure Code (regulated by law 135/2010)

Relevant items	Provisions	Sources used
	b. Treason by disclosure of state secrets - Article 395 Criminal Code c. Treason by helping the enemy - Article 396 Criminal Code d. Actions against constitutional order - Article 397 Criminal Code e. High Treason - Article 398 Criminal Code f. Hostile Actions against the State - Article 399 Criminal Code g. Espionage - Article 400 Criminal Code h. Attempt to jeopardize national security - Article 401 Criminal Code i. Attempt against a community - Article 402 Criminal Code j. Acts of diversion - Article 403 Criminal Code k. Giving false information - Article 404 Criminal Code l. War propaganda - Article 405 Criminal Code m. Compromising State interests - Article 406 Criminal Code n. Disclosure of secrets that endanger national security - Article 407 Criminal Code o. Offences against representatives enjoying international diplomatic immunity - Article 408 Criminal Code p. Creation of illegal intelligence structures - Article 409 Criminal Code q. Failure to report offenses against national security - Article 410 Criminal Code), as well as in case of drug trafficking, weapons trafficking, trafficking in human beings, acts of terrorism, money laundering, counterfeiting of currency or securities, counterfeiting electronic payment instruments, offenses against property, blackmail, rape, deprivation of freedom, tax evasion, corruption offenses and offenses assimilated to corruption, offenses against the European Union's financial interests, offenses committed by means of computer systems or electronic communication devices, or in case of other offenses in respect of which the law sets forth a penalty of no less than 5 years of imprisonment. Electronic surveillance may be ordered in case of: 2) In addition, in case of drug trafficking, weapons trafficking, trafficking in human beings, acts of terrorism, money laundering, counterfeiting of currency or securities, counterfeiting electronic payment instruments, offenses against property, blackmail, rape, illegal deprivation of freedom, tax evasion, corruption offenses and offenses assimilated to corruption, offenses against the European Union's financial interests, offenses committed by means of computer systems or electronic communication devices (most of them have sanctions that prescribe 5 years of imprisonment or more) 3) In addition, any other offence that prescribes 5 years of imprisonment or more	
Does national law allow this tool to be used in cross border cases?	Article 241 (intercepting and recording conversations and communications) from Law 302/2004 allows this tool to be used in cross-border cases.	Article 241, Law 302/2004
What thresholds must be passed for the use of this tool?	The tool can be used for the list of offences described above, or for any other offence that states a term of imprisonment of 5 years or more.	Article 139 (2) Criminal Procedure Code (regulated by law 135/2010)
What types of stakeholder are involved in the implementation of this tool?	The stakeholders involved in the implementation of this tool are the Prosecutor (requests the authorisation), the Judge for Rights and Liberties (authorisation role), criminal investigation bodies or specialised employees of the law enforcement bodies or of other specialist bodies of the state (execution role, may be exercised also by the prosecutor alone), in collaboration with providers of public electronic communication networks or providers of electronic communication services intended for the public or of any other type of communication.	Article 139 (1), Article 140 (1), Article 141, Article 142 (1), (2) Criminal Procedure Code (regulated by law 135/2010)
Which LEAs can use this tool?	The LEAs allowed to use this tool are: 1. Criminal specialised investigation bodies (joint team police - prosecutors): - the Directorate for Investigations of Organised Crime and Terrorism (DIICOT), - - the National Anticorruption Directorate (DNA), 2. Directorate for Combatting Organised Crime- General Inspectorate of the Romanian Police (DCCO) 3. Economic Crimes Investigation Directorate (DICE)	1. OUG 78/2016, approved by law 120/2018, http://legislatie.just.ro/Public/DetaliiDocument/183842 2. OUG 43/2002, http://legislatie.just.ro/Public/DetaliiDocument/35165 3. Law 39/2003, modified by law 255/2013; http://www.cdep.ro/pls/legis/legis_pck.http_act_text?id=39932 4. https://www.politiaromana.ro/ro/politia-romana/unitati-centrale/directia-de-combatere-a-criminalitatii-organizate 4. https://www.politiaromana.ro/ro/politia-romana/unitati-centrale/directia-de-investigare-a-criminalitatii-economice
What are the rules to be followed for the implementation of this tool?	Electronic surveillance covers all the types of surveillance mentioned above. Electronic surveillance is ordered by the Judge for Rights and Liberties, but the request shall mention for which type of surveillance the authorisation is sought, as the case at hand might not require the implementation of all of them. The judge for right and liberties will approve the surveillance when the following requirements are cumulatively met: a) there is a reasonable suspicion in relation to the preparation or commission of one of the offenses listed; b) such measure is proportional to the restriction of fundamental rights and freedoms, considering the particularities of the case, the importance of information or evidence that are to be obtained or the seriousness of the offense; the determination on the proportionality of the measure is conducted on a case-by-case basis (no legal process prescribed), due to the fact that	Article 139 (1), Article 140 (1), (2) Article 144 Criminal Procedure Code (regulated by law 135/2010)

Relevant items	Provisions	Sources used
	the Judge for Rights and Liberties assesses if the request is grounded by considering the particularities of the case at hand; c) evidence could not be obtained in any other way or its obtaining implies special difficulties that would harm the investigation, or there is a threat for the safety of persons or of valuable goods. Electronic surveillance may be ordered during the criminal investigation, for a period of maximum 30 days, upon request by the prosecutor, by the Judge for Rights and Liberties. Such application filed by the prosecutor has to contain: the electronic surveillance measures that are requested for authorisation, the name or the identification data of the person against whom such measure is to be ordered, if known, the evidence or data giving rise to a reasonable suspicion related to the commission of an offense in respect of which such measure may be ordered, the facts and the charges, and, in case of a video, audio or photo surveillance measure, surveillance measure, whether an approval for criminal investigation bodies to enter private spaces indicated for activating and deactivating the technical devices to be used for the enforcement of the electronic surveillance measure is also requested, and a justification of the proportional and subsidiary nature of the measure. The prosecutor has to submit the case file to the Judge for Rights and Liberties. An electronic surveillance warrant may be extended, for well-grounded reasons, by the Judge for Rights and Liberties of the court of competent jurisdiction, upon reasoned request by the prosecutor, in situations where the requirements set by Art. 139 are met; however, each such extension may not exceed 30 days. A 'reasoned request' of the prosecutor in the extension stage must follow the same legal provisions set for the initial request of the prosecutor. Such request must contain the following elements: - the indication of the surveillance measures which are solicited - name or other identification details of the person that is the subject of the surveillance measure - the indication of the evidence or data from which there is a reasonable suspicion in relation to the commission of an offence for which surveillance can be conducted - indication of the offence and of its legal classification - in case the request is made for video, audio or photo surveillance, if it is also requested that the criminal investigation bodies to be allowed to enter indicated private spaces to activate or deactivate the technical devices used in the surveillance - reasoning of the proportional and subsidiary nature of the measure. In practice, the Prosecutorial request for extension must give reasons for why the measure was useful and why it is still necessary in the investigation. Supporting excerpts may be included. If the Judge for Rights and liberties concludes that the conditions are met, he authorizes the extension. Each extension may not exceed 30 days. The total duration of authorised technical surveillance cannot exceed 6 months, for the same individual and same offence in the same case. An exception to this rule is provided by the video, audio or photo surveillance conducted in private spaces, which may not exceed 120 days.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	After the measure has expired, the Prosecutor informs, in written, in maximum 10 days, each subject about the electronic surveillance warrant. After the informing moment, the surveilled individual has the right to request to see the reports that contain the surveillance activities conducted.	Article 145 Criminal Procedure Code
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	For the use of this tool, the authorisation of the Judge for Rights and Liberties is needed. the Judge for Rights and Liberties shall order admission of the prosecutor's application, through a court resolution, and shall issue forthwith an electronic surveillance warrant. The prosecutor may authorize, for a time period of maximum 48 hours, electronic surveillance measures when: - there is an emergency situation, and the obtaining of an electronic surveillance warrant under the terms of Art. 140 would lead to a substantial delay of investigations, to the loss, alteration or destruction of evidence, or would jeopardize the safety of the victim, of witnesses or of their family members; and - the requirements set by Art. 139 par. (1) and (2) are met, requirements which are reiterated below: - Paragraph (1): The Judge for Rights and Liberties will approve the surveillance when the following requirements are cumulatively met: - there is a reasonable suspicion in relation to the preparation or commission of one of the offenses listed; - such measure is proportional to the restriction of fundamental rights and freedoms, considering the particularities of the case, the importance of information or evidence that are to be obtained or the seriousness of the offense; - evidence could not be obtained in any other way or its obtaining implies special difficulties that would harm the investigation, or there is a threat for the safety of persons or of valuable goods.	Article 140 (1), Article 141 (1), (3) Criminal Procedure Code (regulated by law 135/2010)

Relevant items	Provisions	Sources used
	2. Paragraph (2): Electronic surveillance may be ordered in case of offenses against national security stipulated by the Criminal Code and by special laws as well as in case of drug trafficking, weapons trafficking, trafficking in human beings, acts of terrorism, money laundering, counterfeiting of currency or securities, counterfeiting electronic payment instruments, offenses against property, blackmail, rape, deprivation of freedom, tax evasion, corruption offenses and offenses assimilated to corruption, offenses against the European Union's financial interests, offenses committed by means of computer systems or electronic communication devices, or in case of other offenses in respect of which the law sets forth a penalty of no less than 5 years of imprisonment. Within a maximum of 24 hours following expiry of a measure, the prosecutor is under an obligation to notify the Judge for Rights and Liberties, in order for him to confirm the measure and, at the same time, shall forward a report presenting a summary of the electronic surveillance activities performed and the case file. The total duration of an electronic surveillance measure, related to the same person and the same act, may not exceed, in the same case, 6 months, except for the measure of video, audio or photo surveillance in private spaces, which may not exceed 120 days.	
What ongoing supervision is required for the use of this tool?	The prosecutor overseeing the investigation also supervises the implementation of this tool. The prosecutor is under an obligation to request the cease of electronic surveillance before the expiry of the warrant term, if the reasons justifying such measure no longer exist, by immediately informing the judge having issued the warrant.	Article 142 (4) Criminal Procedure Code (regulated by law 135/2010)
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	For matters of national security, the numbers of warrants issues is as follows, from 2017 to 2019: 2019: 1017 2018: 833 2017: 966 The warrants were issued for electronic surveillance, the available data do not specify which particular surveillance activity was authorised.	https://www.mediafax.ro/justitie/inalta-curte-dezvaluie-cate-mandate-de-supraveghere-a-emis-pestes-300-numai-in-primele-luni-din-2020-19226319 https://www.zf.ro/eveniment/cate-mandate-de-supraveghere-a-emis-anul-acesta-inalta-curte-de-19226315
Undercover / covert operations		
Relevant documents (legal and non-legal) that define the functioning of the tool	Article 138 (1) g), art. 148 Criminal Procedure Code (both regulated by law 135/2010)	Article 138 (1) g), art. 148 Criminal Procedure Code (both regulated by law 135/2010)
How is the tool defined?	Use of undercover investigators and collaborators designates the use of a person with an identity other than their real one, for the purpose of obtaining data and information regarding the commission of an offense.	Article 138 (1) g) Criminal Procedure Code (regulated by law 135/2010)
For what types of crime can the tool be used?	The use of undercover/covert operations can be used for offenses against national security set forth by the Criminal Code and by other special laws, as well as in case of offenses of drug trafficking, weapons trafficking, trafficking in human beings, acts of terrorism or acts assimilated to those, terrorism financing, money laundering, counterfeiting of currency or other securities, counterfeiting of electronic payment instruments, blackmail, deprivation of freedom, tax evasion, corruption offenses, offenses assimilated to corruption offenses, offenses against the European Union's financial interests, of offenses committed by means of a computer systems or electronic communication devices, or in case of other offenses in respect of which the law requires a penalty of no less than 7 years of imprisonment, or when there is a reasonable suspicion that a person is involved in criminal activities that are related to the above-mentioned offenses. The use of undercover/covert operations can be employed in the following cases: 1. There is a reasonable suspicion that the following offences are in preparation or are committed: a) offences against national security set forth by the Criminal Code and by other special laws (already listed above) b) offences of drug trafficking, weapons trafficking, human trafficking and exploiting (vulnerable individuals), acts of terrorism or acts assimilated to those, terrorism financing, money laundering, counterfeiting of currency or other securities, counterfeiting of electronic payment instruments, blackmail, illegal deprivation of freedom, tax evasion, corruption offenses, offenses assimilated to corruption offenses, offenses against the European Union's financial interests, of offenses committed by means of a computer systems or electronic communication devices c) in case of other offences for which the law prescribes a penalty of 7 years imprisonment or more OR	Article 148 (1) a) Criminal Procedure Code (regulated by law 135/2010)

Relevant items	Provisions	Sources used
	2. There is a reasonable suspicion that a person is involved in criminal activities that relate to the above-mentioned offences.	
Does national law allow this tool to be used in cross border cases?	Article 238 (Law 302/2004) allows the use of this tool in cross-border cases.	Article 238, law 302/2004
What thresholds must be passed for the use of this tool?	The tool can be used for the list of offences described above, or for any other offence that states a term of imprisonment of 7 years or more.	Article 148 (1) a) Criminal Procedure Code (regulated by law 135/2010)
What types of stakeholder are involved in the implementation of this tool?	The stakeholders involved in the implementation of the tool are the Prosecutor (authorisation role), the undercover investigators (intelligence employees within the judicial police, execution role), collaborators and the Judge for Rights and Liberties in case electronic surveillance is necessary (authorisation role). In case of investigation of offenses against national security and of terrorism offenses, intelligence employees within the state bodies performing, under the law, intelligence activities for ensuring national security, can be also used as undercover investigators.	Article 148(1),(3), (4), (10) Criminal Procedure Code (regulated by law 135/2010)
Which LEAs can use this tool?	The LEAs allowed to use this tool are: 1. Criminal specialised investigation bodies (joint team police - prosecutors): - the Directorate for Investigations of Organised Crime and Terrorism (DIICOT), - - the National Anticorruption Directorate (DNA), 2. Directorate for Combatting Organised Crime- General Inspectorate of the Romanian Police (DCCO) 3. Economic Crimes Investigation Directorate (DICE)	1. OUG 78/2016, approved by law 120/2018, http://legislatie.just.ro/Public/DetaliiDocument/183842 2. OUG 43/2002, http://legislatie.just.ro/Public/DetaliiDocument/35165 3. Law 39/2003, modified by law 255/2013; http://www.cdep.ro/pls/legis/legis_pck.http_act_text?id=39932 - https://www.politiaromana.ro/ro/politia-romana/unitati-centrale/directia-de-combatere-a-criminalitatii-organizate 4. https://www.politiaromana.ro/ro/politia-romana/unitati-centrale/directia-de-investigare-a-criminalitatii-economice
What are the rules to be followed for the implementation of this tool?	Authorisation of the use of undercover investigators may be ordered by the prosecutor supervising or conducting the criminal investigation, for a time period of maximum 60 days, if: a) there is a reasonable suspicion related to the preparation or commission of an offense against national security set forth by the Criminal Code and by other special laws, as well as in case of offenses of drug trafficking, weapons trafficking, trafficking in human beings, acts of terrorism or acts assimilated to those, terrorism financing, money laundering, counterfeiting of currency or other securities, counterfeiting of electronic payment instruments, blackmail, deprivation of freedom, tax evasion, corruption offenses, offenses assimilated to corruption offenses, offenses against the European Union's financial interests, of offenses committed by means of a computer systems or electronic communication devices, or in case of other offenses in respect of which the law requires a penalty of no less than 7 years of imprisonment, or when there is a reasonable suspicion that a person is involved in criminal activities that are related to the above-mentioned offenses; b) such measure is necessary and proportional to the restriction of fundamental rights and freedoms, considering the particularities of the offense, the importance of information or of evidence to be obtained, or the seriousness of the offense; c) evidence or the offender's, the suspect's or defendant's localisation or identity could not be obtained in other way or obtaining it would imply extreme difficulties that would harm the investigation, or there is a threat to the safety of persons or of high value goods. the total duration of such measure, in the same case and in respect of the same person, may not exceed one year, except for offenses against life, national security, drug trafficking, weapons trafficking, and trafficking in person, acts of terrorism, money laundering, as well as for offenses against the European Union's financial interests.	Article 148 (1), (9) Criminal Procedure Code (regulated by law 135/2010)
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	According to Article 149 Criminal Procedure Code, the real identity of the undercover investigators and of collaborators with a different identity than their real one cannot be disclosed. The identities are only known by the Prosecutor, Judge for Rights and Liberties, the Preliminary Room Judge and the Court. The undercover investigator, the collaborators, informant, as well as their family members can benefit from special measures for witness protection.	Article 149, Criminal Procedure Code (Law 135/2010)
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Such measure is ordered by the prosecutor, ex officio or upon request by criminal investigation bodies, through an order that needs to include the following: a) the activities an undercover investigator is authorised to perform; b) the time interval for which the measure was authorised; c) the identity awarded to the undercover investigator. If the prosecutor deems it necessary for the undercover investigator to be able to use technical devices in order to obtain pictures or audio and video recordings, they shall notify the Judge for Rights and Liberties requesting an electronic surveillance warrant.	Article 148 (1), (3) Criminal Procedure Code (regulated by law 135/2010)
What ongoing supervision is required for the use of this tool?	Ongoing supervision for the use of this tool is ensured by the Prosecutor who oversees the criminal investigation.	Article 148 (1) Criminal Procedure Code (regulated by law 135/2010)

Relevant items	Provisions	Sources used
	The information available does not provide an answer to this inquiry.	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	Article 2, point 4 d), Article 21 from Law 39/2003, last modified through Law 255/2013	Article 2, point 4 d), Article 21 from Law 39/2003, last modified through Law 255/2013
Specific range of application of the tool	An informant is defined as a person who has knowledge of an Organised Criminal Group and gives information or relevant data to the judicial bodies, in order to prevent, uncover or to sanction the perpetration of an offence by one or more members of the Group.	Article 2 from Law 39/2003, last modified through Law 255/2013
How is the tool defined?	In exceptional situations, if there are thorough clues that an offence has been committed or that is in preparation of being committed, by one or more members of an organised criminal group, which cannot be uncovered or whose authors cannot be identified through other means, the use of informants is allowed, in order to gather data regarding the identification of the perpetrators or the offence.	Article 21 from Law 39/2003, last modified through Law 255/2013
For what types of crime can the tool be used?	Law 39/2003 covers the following offences: organised crime groups, offences for which the punishment is life in prison or 4 years or more imprisonment, transnational offences ("cross crime areas")	Article 2 from Law 39/2003, last modified through Law 255/2013
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	The tool can be used for the list of offences described above, or for any other offence that states a term of imprisonment of 4 years or more.	Article 2 from Law 39/2003, last modified through Law 255/2013 for the implementation of the Romanian Criminal Procedure Law
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	Only the judicial police is allowed to use informants.	1. OUG 78/2016, approved by law 120/2018, http://legislatie.just.ro/Public/DetaliiDocument/183842 2. OUG 43/2002, http://legislatie.just.ro/Public/DetaliiDocument/35165 3. Law 39/2003, modified by law 255/2013; http://www.cdep.ro/pls/legis/legis_pck.htp_act_text?id=39932 4. https://www.politiaromana.ro/ro/politia-romana/unitati-centrale/directia-de-combatere-a-criminalitatii-organizate 4. https://www.politiaromana.ro/ro/politia-romana/unitati-centrale/directia-de-investigare-a-criminalitatii-economice
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	Article 2, point 4 d), Article 21 from Law 39/2003, last modified through Law 255/2013	Article 2, point 4 d), Article 21 from Law 39/2003, last modified through Law 255/2013
Authorised participation in specific activities		
Relevant documents (legal and non-legal) that define the functioning of the tool	Article 138 (1) h), Article 150 Criminal Procedure Code (both regulated by law 135/2010)	Article 138 (1) h), Article 150 Criminal Procedure Code (both regulated by law 135/2010)

Relevant items	Provisions	Sources used
How is the tool defined?	Authorised participation in specific activities means the commission of acts similar to the objective component of a corruption offense, the performance of transactions, operations or any other kind of arrangements related to an asset or to a person who is presumed missing, a victim of trafficking in human beings or of kidnapping, the performance of operations involving drugs, as well as the providing of services, based on an authorisation from the judicial bodies of competent jurisdiction for the purpose of obtaining evidence. The individual that is authorised through a Prosecutorial Order by the Prosecutor will conduct the indicated authorised activities (found in the Prosecutorial Order). These activities do not constitute contraventions or offences, even if they represent the objective component of offences. The judiciary bodies can use or put at the disposal of the individual any written document or object necessary to conduct the authorised activity. The individual may be subject to a hearing as a witness during the criminal trial (as a threatened witness). The purpose of this tool is to obtain evidence.	Article 138 (1) h) Criminal Procedure Code (regulated by law 135/2010) , art 150
For what types of crime can the tool be used?	This tool can be used for drug trafficking, weapons trafficking, trafficking in human beings, acts of terrorism or acts assimilated to those, terrorism financing, money laundering, counterfeiting of currency or other securities, counterfeiting of electronic payment instruments, blackmail, deprivation of freedom, tax evasion, corruption offenses, offenses assimilated to corruption offenses, offenses against the European Union's financial interests, of offenses committed by means of a computer systems or electronic communication devices, or in case of other offenses in respect of which the law requires a penalty of no less than 7 years of imprisonment, or when there is a reasonable suspicion that a person is involved in criminal activities that are related to the above-mentioned offenses.	Article 150 (1) a) Criminal Procedure Code (regulated by law 135/2010)
Does national law allow this tool to be used in cross-border cases?	N/A	
What thresholds must be passed for the use of this tool?	This tool can be used for the above mentioned offences or for any other offence that states a term of imprisonment of 7 years or more.	Article 150 (1) a) Criminal Procedure Code (regulated by law 135/2010)
What types of stakeholder are involved in the implementation of this tool?	The stakeholders involved in the implementation of this tool are the Prosecutor (authorisation role), criminal investigation bodies (execution role), in collaboration with investigators with real identities, undercover investigators, collaborators.	Article 150 (1) a), (3) Criminal Procedure Code (regulated by law 135/2010)
Which LEAs can use this tool?	The LEAs allowed to use this tool are: 1. Criminal specialised investigation bodies (joint team police - prosecutors): - the Directorate for Investigations of Organised Crime and Terrorism (DIICOT), - - the National Anticorruption Directorate (DNA), 2. Directorate for Combatting Organised Crime- General Inspectorate of the Romanian Police (DCCO) 3. Economic Crimes Investigation Directorate (DICE) The individuals who carry out the activities are: a) staff of the above mentioned Agencies (which represent criminal investigation bodies), category which also contains investigators with real identity or under cover b) collaborators, which can operate under their real identity or under cover c) informants may be used; for example, in the case of bribery whistle-blowers, which are then used in a similar authorised activity in order to gather evidence from the other individuals involved in the bribery	1. OUG 78/2016, approved by law 120/2018, http://legislatie.just.ro/Public/DetaliiDocument/183842 2. OUG 43/2002, http://legislatie.just.ro/Public/DetaliiDocument/35165 3. Law 39/2003, modified by law 255/2013; http://www.cdep.ro/pls/legis/legis_pck.htm_act_text?id=39932 4. https://www.politiaromana.ro/ro/politia-romana/unitati-centrale/directia-de-combatere-a-criminalitatii-organizate 4. https://www.politiaromana.ro/ro/politia-romana/unitati-centrale/directia-de-investigare-a-criminalitatii-economice
What are the rules to be followed for the implementation of this tool?	Authorised participation in specific activities may be ordered by the prosecutor supervising or conducting the criminal investigation, for a time period of maximum 60 days, if: a) there is a reasonable suspicion related to the preparation or commission of the above-mentioned offenses b) such measure is necessary and proportional to the restriction of fundamental rights and freedoms, considering the particularities of the offense, the importance of information or of evidence to be obtained or the seriousness of the offense; c) evidence could not be obtained in other way or obtaining it would imply extreme difficulties that would harm the investigation, or there is a threat for the safety of persons or of high value goods.	Article 150 Criminal Procedure Code (regulated by law 135/2010)
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool?(e.g. senior police officer, prosecutor, judge, other)	Such measure is ordered by the prosecutor, ex officio or upon request by criminal investigation bodies, through an order that needs to include, the following: a) the activities authorised to be performed; b) the duration for which the measure was authorised; c) the person performing the authorised activities. The individuals who carry out the activities are:	Article 150 Criminal Procedure Code (regulated by law 135/2010)

Relevant items	Provisions	Sources used
	a) staff of the above mentioned Agencies (which represent criminal investigation bodies), category which also contains investigators with real identity or under cover b) collaborators, which can operate under their real identity or under cover c) informants may be used; for example, in the case of bribery whistle-blowers, which are then used in a similar authorised activity in order to entrap the other individuals involved in the bribery An ordered measure may be extended by the prosecutor, for well-grounded reasons, provided that the requirements set by par. (1) are met; however, each such extension may not exceed 60 days. The total duration of such measure may not exceed one year in respect of the same person and the same act.	
What ongoing supervision is required for the use of this tool?	Ongoing supervision for the use of this tool is ensured by the Prosecutor who oversees the criminal investigation. The available information does not supply an answer to this inquiry. The Prosecutor oversees the entire criminal investigation, which includes all criminal investigation tools, including the participation in authorised activities.	Article 150 Criminal Procedure Code (regulated by law 135/2010)
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Obtaining data generated or processed by providers of public electronic communications networks or providers of electronic communication services intended for the public, other than the content of communications, and stored by these		
Relevant documents (legal and non-legal) that define the functioning of the tool	Article 138 (1) j), Article 152 Criminal Procedure Code (both regulated by law 135/2010)	Article 138 (1) j), Article 152 Criminal Procedure Code (both regulated by law 135/2010)
How is the tool defined?	Obtaining data generated or processed by providers of public electronic communications networks or providers of electronic communication services intended for the public, other than the content of communications, and stored by these	Article 138 (1) j) Criminal Procedure Code (regulated by law 135/2010)
For what types of crime can the tool be used?	This tool may be ordered in case of offenses against national security stipulated by the Criminal Code and by special laws, as well as in case of drug trafficking, weapons trafficking, trafficking in human beings, acts of terrorism, money laundering, counterfeiting of currency or securities, counterfeiting electronic payment instruments, offenses against property, blackmail, rape, deprivation of freedom, tax evasion, corruption offenses and offenses assimilated to corruption, offenses against the European Union's financial interests, offenses committed by means of computer systems or electronic communication devices, or in case of other offenses in respect of which the law sets forth a penalty of no less than 5 years of imprisonment. (cross crime areas)	Article 152 (1) a) Criminal Procedure Code (regulated by law 135/2010)
Does national law allow this tool to be used in cross-border cases?	N/A	
What thresholds must be passed for the use of this tool?	The tool can be used for the list of offences described above, or for any other offence that states a term of imprisonment of 5 years or more.	Article 152 (1) a) Criminal Procedure Code (regulated by law 135/2010)
What types of stakeholder are involved in the implementation of this tool?	The stakeholders involved in the implementation of this tool are the Judge for Rights and Liberties (authorisation role) , criminal investigation bodies (execution role), in collaboration with providers of public electronic communication networks, providers of electronic communication services intended for the public, other than the content of communications.	Article 152 (1), (3) Criminal Procedure Code (regulated by law 135/2010)
Which LEAs can use this tool?	The LEAs allowed to use this tool are: 1. Criminal specialised investigation bodies (joint team police - prosecutors): - the Directorate for Investigations of Organised Crime and Terrorism (DIICOT), - - the National Anticorruption Directorate (DNA), 2. Directorate for Combatting Organised Crime- General Inspectorate of the Romanian Police (DCCO) 3. Economic Crimes Investigation Directorate (DICE)	1. OUG 78/2016, approved by law 120/2018, http://legislatie.just.ro/Public/DetaliiDocument/183842 2. OUG 43/2002, http://legislatie.just.ro/Public/DetaliiDocument/35165 3. Law 39/2003, modified by law 255/2013; http://www.cdep.ro/pls/legis/legis_pck.http_act_text?id=39932 4. https://www.politiaromana.ro/ro/politia-romana/unitati-centrale/directia-de-combatere-a-criminalitatii-organizate 4. https://www.politiaromana.ro/ro/politia-romana/unitati-centrale/directia-de-investigare-a-criminalitatii-economice
What are the rules to be followed for the implementation of this tool?	Criminal investigation bodies, based on a prior authorisation from the Judge for Rights and Liberties, may request a provider of public electronic communication networks or a provider of electronic communication services intended for the public to transmit the data stored by it, if the following conditions are met: a) there is a reasonable suspicion related to the commission of one of the offenses listed b) there are reasonable ground to believe that the requested data may constitute evidence	Article 152 Criminal Procedure Code (regulated by law 135/2010)

Relevant items	Provisions	Sources used
	c) evidence could not be obtained in other way or obtaining it would imply extreme difficulties that would harm the investigation, or there is a threat for the safety of persons or of high value goods c) such measure is necessary and proportional to the restriction of fundamental rights and freedoms, considering the particularities of the offense, the importance of information or of evidence to be obtained or the seriousness of the offense	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool?(e.g. senior police officer, prosecutor, judge, other)	The Judge for Rights and Liberties provides the authorisation for the use of this tool within 48 hours.	Article 152 (2) Criminal Procedure Code (regulated by law 135/2010)
What ongoing supervision is required for the use of this tool?	Ongoing supervision for the use of this tool is ensured by the Prosecutor who oversees the criminal investigation.	Article 152 (1) Criminal Procedure Code (regulated by law 135/2010)
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Relevant documents (legal and non-legal) that define the functioning of the tool	Article 138 (1) f), Article 147 Criminal Procedure Code (both regulated by law 135/2010)	Article 138 (1) f), Article 147 Criminal Procedure Code (both regulated by law 135/2010)
How is the tool defined?	Search of mail deliveries designates the inspection, through physical or technical methods, of letters or other mail deliveries or objects transmitted through any other means.	Article 138 (1) f) Criminal Procedure Code (regulated by law 135/2010)
For what types of crime can the tool be used?	This tool may be ordered in case of offenses against national security stipulated by the Criminal Code and by special laws, as well as in case of drug trafficking, weapons trafficking, trafficking in human beings, acts of terrorism, money laundering, counterfeiting of currency or securities, counterfeiting electronic payment instruments, offenses against property, blackmail, rape, deprivation of freedom, tax evasion, corruption offenses and offenses assimilated to corruption, offenses against the European Union's financial interests, offenses committed by means of computer systems or electronic communication devices, or in case of other offenses in respect of which the law sets forth a penalty of no less than 5 years of imprisonment. (cross crime areas)	Article 147 (2) Criminal Procedure Code (regulated by law 135/2010)
Does national law allow this tool to be used in cross-border cases?	N/A	
What thresholds must be passed for the use of this tool?	The tool can be used for the list of offences described above, or for any other offence that states a term of imprisonment of 5 years or more.	Article 147 (2) Criminal Procedure Code (regulated by law 135/2010)
What types of stakeholder are involved in the implementation of this tool?	The stakeholders involved in the implementation of this tool are the Prosecutor (initiates request), the Judge for Rights and Liberties (authorisation role), in collaboration with postal or transport entities and any other natural persons or legal entities performing transport or information transfer activities.	Article 147 (1), (5) Criminal Procedure Code (regulated by law 135/2010)
Which LEAs can use this tool?	The LEAs allowed to use this tool are: 1. Criminal specialised investigation bodies (joint team police - prosecutors): - the Directorate for Investigations of Organised Crime and Terrorism (DIICOT), - - the National Anticorruption Directorate (DNA), 2. Directorate for Combatting Organised Crime- General Inspectorate of the Romanian Police (DCCO) 3. Economic Crimes Investigation Directorate (DICE)	1. OUG 78/2016, approved by law 120/2018, http://legislatie.just.ro/Public/DetaliiDocument/183842 2. OUG 43/2002, http://legislatie.just.ro/Public/DetaliiDocument/35165 3. Law 39/2003, modified by law 255/2013; http://www.cdep.ro/pls/legis/legis_pck.htm_act_text?id=39932 4. https://www.politiaromana.ro/ro/politia-romana/unitati-centrale/directia-de-combatere-a-criminalitatii-organizate 4. https://www.politiaromana.ro/ro/politia-romana/unitati-centrale/directia-de-investigare-a-criminalitatii-economice
What are the rules to be followed for the implementation of this tool?	Withholding, surrender and search of postal deliveries may be ordered by the Judge for Rights and Liberties in respect of letters, postal dispatches or items sent or received by a perpetrator, suspect, defendant or by any person suspected to receive or send, by any means, such goods from/to a perpetrator, suspect or defendant, or goods intended to it, if: a) there is a reasonable suspicion related to the preparation or commission of an offense; b) such step is necessary and proportional to the restriction of fundamental rights and freedoms, considering the particularities of the case, the importance of information or of evidence to be obtained or the offense seriousness;	Article 147 (1) Criminal Procedure Code (regulated by law 135/2010)

Relevant items	Provisions	Sources used
	c) evidence could not be obtained in other way, or obtaining it would imply extreme difficulties that would harm the investigation or there is a threat against the safety of persons or of high value goods.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool?(e.g. senior police officer, prosecutor, judge, other)	The authorisation of the Judge for Rights and Liberties is needed, upon request of the Prosecutor. In emergency situations, when the obtaining of a warrant for the withholding, surrender and search of postal deliveries under general procedure would result in a substantial delay of the investigations, in the loss, alteration or destruction of evidence or would endanger the safety of the victim or of other persons, and the requirements set by the general procedure are met, the prosecutor may order, for a term of maximum 48 hours, the measures in question. Within a maximum of 24 hours following expiry of a measure, the prosecutor is under an obligation to notify the Judge for Rights and Liberties , in order for him to confirm the measure.	Article 147 (1), (4) Criminal Procedure Code (regulated by law 135/2010)
What ongoing supervision is required for the use of this tool?	Ongoing supervision for the use of this tool is ensured by the Prosecutor who oversees the criminal investigation.	Article 147 (1), Criminal Procedure Code (regulated by law 135/2010)
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	

Source: Author's own elaboration

Slovenia

Table 44 – Overview of national rules on investigative tools - Slovenia

Relevant items	Provisions	Sources used
Controlled Delivery		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Procedure Act (ZKP), Official Gazette no. 32/12 – consolidated version, no. 47/13, 87/14, 8/16 – Constitutional Court decision, 64/16 – Constitutional Court decision, 65/16 – Constitutional Court decision, 66/17 – ORZKP153,154, 22/19, 55/20 - Constitutional Court decision, 89/20 - Constitutional Court decision, 191/20 - Constitutional Court decision and no. 200/20) Cooperation in Criminal Matters with the Member States of the European Union Act (ZSKZDČEU-1), Official Gazette of Republic of Slovenia no. 48/13, 37/15 in 22/18 Agreement between the Republic of Slovenia and the Republic of Austria on Police Cooperation (BATPS) Agreement between the Republic of Slovenia and the Republic of Hungary on cross-border co-operation of law enforcement authorities (BHUČPS) Agreement between the Republic of Slovenia and the Republic of Italy on cross-border police cooperation (BITČPS) Agreement between the Republic of Slovenia and the Republic of Croatia on Cross-border police co-operation (BHRPS) Police Cooperation Convention for Southeast Europe (Official Gazette of Republic of Slovenia no. 18/12) (MKPS)	- ZKP (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362# - ZKP (English - not all changes and amendments are included) https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf - Cooperation Act (Slovenian): http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6513 - Cooperation Act (English): https://www.ejtn.eu/PageFiles/6533/2014%20seminars/Nicosia/SI_Legislation/Law_Cooperation_Criminal_Matters.pdf - BATPS (Slovenian & German): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2004-02-0052/#I.%C2%A0poglavjeSplo%C5%A1ne%C2%A0dolo%C4%8Dbe - BHUČPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0029?sop=2007-02-0029 - BITČPS (Slovenian & Italian): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0134?sop=2007-02-0134 - BHRPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2003-02-0014?sop=2003-02-0014 - MKPS (English) https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2012-02-0103/zakon-o-ratifikaciji-konvencije-o-policijskem-sodelovanju-v-jugovzhodni-evropi-mkps - For parties to the police cooperation convention see https://www.pccseesecretariat.si/index.php?page=documentspcc&item=35
How is the tool defined?	Article 55 of ZSKZDČEU-1 (1) Controlled delivery shall mean an agreed covert surveillance of transport or the transfer of persons, items or goods the trade in which is limited or prohibited, to, from or through the territory of the Republic of Slovenia, where the competent authorities, for the purpose of revealing a large-scale criminal activity, temporarily postpone the execution of the deprivation of liberty and other measures provided by the law governing criminal procedure.	- ZKP (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362# - ZKP (English - not all changes and amendments are included) https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf - Cooperation Act (Slovenian): http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6513

Relevant items	Provisions	Sources used
	(2) Rendering a decision on controlled delivery shall fall within the competences of a district state prosecutor through whose area of authority the controlled delivery is envisaged to cross the state border, or from the area of whom it is dispatched, or a Specialised Office of the State Prosecutor of the Republic of Slovenia. (3) A controlled delivery shall be permitted at the request of a competent authority of a Member State, or in agreement with another Member State, if criminal offences are involved which meet the conditions for issuing a European Arrest Warrant. (4) In the territory of the Republic of Slovenia, controlled delivery shall be exercised by the competent Slovenian authorities in a manner which ensures permanent supervision and appropriate action. (5) Controlled delivery shall not be permitted, or its further execution shall be discontinued if: 1. or until there is a risk to people's life or health; or 2. it is likely that further supervision or action in another Member State is not ensured or will not be effective. (6) After the execution of a controlled delivery, a competent state prosecutor must establish that the conditions exist for referring criminal prosecution to the Member State in which suspects have been deprived of liberty. In this regard Article 159 of Criminal Procedure Code (ZKP) is relevant: The arrest of a suspect and the execution of other measures provided by this Act may be temporarily postponed with a view to discovering a major criminal activity but only if, and as long as, the lives and health of third persons are not thereby endangered. Permission to postpone these measures shall upon a properly reasoned proposal by the internal affairs agency be granted by the public prosecutor with appropriate jurisdiction. Article 11 of BATPS (1) At the request of the requesting Contracting Party, the requested Contracting Party may authorize controlled imports into its territory, controlled transit or controlled exports, in particular in the case of illicit trafficking in narcotic drugs, arms, explosives, counterfeit money, stolen goods and concealment and money laundering if the disclosure of end-customer and other participants or the discovery of distribution channels would otherwise be unsuccessful or substantially difficult in the opinion of the requesting Party. The controlled delivery may, by agreement between the Parties, be intercepted and handed over for further carriage so as to remain intact, to be removed or replaced in whole or in part. If the goods present an unacceptable risk to the persons involved in their transport or endanger public safety, the requested Contracting Party shall restrict or refuse the controlled shipment. (2) In order to prevent the interruption of control, the requested Contracting Party shall take control of the delivery upon crossing the state border. During further transport, it ensures its constant control in a form that allows the perpetrators to be arrested or the goods seized at any time. Officials of the requesting Contracting Party may, in agreement with the requested Contracting Party, continue to accompany the controlled delivery after its acceptance together with the officials of the requested Contracting Party who took over the delivery, but without exercising official authority. In so doing, they shall be bound by the provisions of this Article and the national law of the requested Contracting Party and shall be bound by the orders of the authorities of the requested Contracting Party. (3) Requests for controlled delivery commencing or continuing in a State which is not a party to this Treaty shall be granted only if it is ensured that that State meets the conditions under the first and second sentences of the second paragraph of this Article. (4) Points c, d, e, h, i and j of the fifth paragraph of Article 7 of this Agreement shall apply mutatis mutandis to the execution of a controlled consignment. (5) Requests pursuant to the first paragraph of this Article shall be addressed in the Republic of Slovenia to the Ministry of the Interior, the General Police Administration, the Criminal Police Administration, in the Republic of Austria to the Federal Ministry of the Interior, the Directorate-General for Public Security, the Federal Criminal Bureau, and in the case of controlled exports to the Public Prosecutor's Office in whose official district the transport begins, at the same time notifying the Federal Ministry of the Interior. Paragraph 5., Article 7 (in relation to the paragraph 4. of Article 11 BATPS) 5) Covert surveillance and tracking in accordance with the first and third paragraphs of this Article is permitted only under the following conditions: c) officials carrying out covert surveillance must always be able to prove their official function; d) officials carrying out covert surveillance and surveillance may carry their service weapons during such surveillance, unless the requested Party expressly objects. The use of weapons is only allowed in the self-defence; e) entry into apartments and publicly inaccessible land is not allowed. Entry into publicly accessible working, operating and business premises is possible during their working, operating and business hours;	• Cooperation Act (English): https://www.ejtn.eu/PageFiles/6533/2014%20seminars/Nicosia/SI_Legislation/Law_Cooperation_Criminal_Matters.pdf • BATPS (Slovenian & German): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2004-02-0052/#I.%C2%A0poglavjeSplo%C5%A1ne%C2%A0dolo%C4%8Dbe • BHUCPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0029?sop=2007-02-0029 • BITCPS (Slovenian & Italian): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0134?sop=2007-02-0134 • MKPS https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2012-02-0103/zakon-o-ratifikaciji-konvencije-o-policijskem-sodelovanju-v-jugovzhodni-evropi-mkps

Relevant items	Provisions	Sources used
	h) the authorities of the Contracting Party from which the secret surveillance and tracking officials come shall, upon request, provide support for the subsequent investigation, including the legal proceedings of the Contracting Party in whose territory the covert surveillance and tracking took place; i) the technical means necessary to carry out covert surveillance and surveillance may be used to the extent necessary in accordance with the national law of the Contracting Party in whose territory it is carried out. The technical means used for covert surveillance and tracking must be specified in the request referred to in the first paragraph of this Article; j) the vehicles used are, in terms of exemption from traffic bans and traffic restrictions, equivalent to those of the security authorities of the Contracting Party in whose territory they are used. Signalling may be used if necessary for the purpose of conducting covert surveillance and tracking. Article 13 of BHUČPS 1. Based on request, the authorised co-operating authorities of the Contracting Parties shall enable controlled delivery within the territory of their own states in accordance with the conditions set forth in this Article. Controlled delivery is a covert activity of the authorised co-operating authorities, in the course of which – within the framework of international co-operation – they enable the passing of a thing in possession of a person subject to surveillance to and from the territory of the Contracting Parties to another state and its transit through the territory of the Contracting Parties with a view to enabling the detection of criminal acts and the identification of persons participating in the perpetration of criminal acts in the widest range possible. 2. In addition to the data set forth in Article 4 (1) of this Agreement, the request sent to the central contact points for controlled delivery shall include: a) the content of the consignment, the expected route of travel, the time frame and means of transportation, the information enabling the identification of a vehicle; b) the mode of escort; c) the technical instruments to be used; d) the number of participants in the escort on the part of the requesting Contracting Party; e) the mode of maintaining contact with the participants of the controlled delivery; f) the circumstances of handing over and taking over the consignment; g) the measures to be carried out upon arrest; h) the measures to be carried out in unexpected circumstances. 3. If the delay could pose a risk or threaten the interests of crime suppression activities, the request for controlled delivery may be directly sent or received by the authorised co-operating authorities. Such a request shall be sent subsequently as soon as possible to the central contact points of the Contracting Parties. The request shall contain documents substantiating controlled delivery. 4. The authorised co-operating authorities shall agree on the date and modus operandi of the controlled delivery and the extent of their involvement on each occasion. The authorised co-operating authority of the requested Contracting Party may restrict or refuse controlled delivery if it could endanger the persons participating in it or public security to an unacceptable extent. 5. The authorised co-operating authority of the requested Contracting Party shall be in command of the controlled delivery; the requesting Contracting Party shall be informed of the person in charge. The controlled delivery shall be carried out in a manner that will allow easy interception at any time. Following takeover, the authorised co-operating authority of the requesting Contracting Party may escort the consignment but may not exercise official powers. In the course of this, the authorised co-operating authority of the requesting Contracting Party shall act in accordance with the provisions of this Article, the laws and regulations of the requested Contracting Party and the instructions of the person in charge of the authorised co-operating authority of the requested Contracting Party. 6. The Contracting Parties shall also enable the execution of controlled deliveries starting out from a third country to a further country. In this case, the requesting Contracting Party shall obtain the prior authorisation of the states concerned, of which the requested Contracting Party shall be notified. 7. The participation of an undercover agent in the controlled delivery is possible only with the authorisation of the judicial authorities of the Contracting Party which is using the undercover agent. Paragraph 1., Article 4 (in relation to the paragraph 13. of Article 11 BHUČPS) 1. Unless otherwise specified in this Agreement, the request shall include at least: a) the name of the requesting authorised co-operating authority; b) the subject of the request; c) the description and legal qualification of the act to which the request refers; d) the time limit set for the fulfilment of the request and grounds for the degree of urgency; e) where necessary, the authorisation of the judicial authorities;	

Relevant items	Provisions	Sources used
	f) the request to involve a member of the authorised co-operating authority of the requesting Contracting Party in the execution of the request, if so requested by the requesting Contracting Party; g) identification data of the person concerned, if known, to the extent necessary for the execution of the request. Article 10 of BITČPS 1. Subject to the laws in force in both Contracting Parties and subject to prior detailed arrangements to be made between the competent authorities, the Contracting Parties undertake to facilitate and provide assistance in carrying out "controlled delivery" and the "covert operation". 2. The request referred from the previous paragraph must be sent: - in the Republic of Slovenia: the Ministry of the Interior, the Police, the General Police Administration, the Criminal Police Administration; - in the Italian Republic: the Ministry of the Interior, the Public Security Administration, the Central Directorate for the Fight against Drugs and for activities relating to investigations into drugs and psychotropic substances and precursors. The Central Directorate of the Criminal Police - International Police Cooperation Service is responsible for the remaining request. Nothing is written in the agreement between Croatia and Slovenia on cross-border police cooperation on controlled delivery, so the laws of both countries are taken into account. Article 15 of MKPS (1) Upon Letter of Request from a Contracting Party, another Contracting Party can, in case of investigations for extraditable offences, if appropriate, permit controlled delivery on its territory, especially of transport of narcotic drugs, precursors, firearms, explosives, counterfeit currency, and items originating from a crime, or intended to be used to commit a crime, if the requesting Contracting Party explains that, without such a measure, identification of perpetrators or of distributing routes would be impossible or extremely hampered. If the content of a controlled delivery presents a particular risk for the persons involved, or a danger to the public, the requested Contracting Party has the right to ask that certain conditions to be met before granting the request or refuse the request altogether. (2) The requested Contracting Party shall take control over the delivery when it crosses the border, or at a place of taking over agreed by the law enforcement authorities, in order to avoid interruption of control, and guarantees permanent surveillance of the shipment in a manner that enables police intervention at any time. After takeover by the requested Contracting Party, officers of the requesting Contracting Party can continue to follow the controlled delivery together with officers of the requested Contracting Party, upon agreement with the requested Contracting Party. (3) The officers of the requesting Contracting Party are obliged to observe the laws of the requested Contracting Party. (4) If the competent law enforcement authorities of the requested Contracting Party cannot intervene in due time, and if continuation of the controlled delivery would present a serious risk for life or health of persons, or cause serious damage to property, or if the delivery could no longer be kept under control, the officer of the requesting Contracting Party can seize the controlled delivery. If necessary, the officers of the requesting Contracting Party can stop and apprehend persons who escort the shipment until intervention by law enforcement authorities of the requested Contracting Party. In any case the requesting Contracting Party shall inform the law enforcement authorities of the requested Contracting Party without delay. (5) When a controlled delivery has been seized on the territory of the requested Contracting Party, it may be handed over to the requesting Contracting Party on the basis of a Letter of Request. (6) A person who, following the action provided for in paragraph 4, has been arrested by the competent local authorities may, whatever that person's citizenship, be held for questioning. The relevant rules of national law shall apply mutatis mutandis. (7) If the person is not a national of the Contracting Party in whose territory he/she was arrested, that person shall be released no later than six hours after the arrest was made, not including the hours between midnight and 9.00 a.m., unless the competent local authorities have previously received a request for that person's provisional arrest for the purposes of extradition in any form whatsoever. (8) In the course of a controlled delivery, the provisions of Article 14, paragraph 5, sub-paragraph a) to c) and e) to h) shall apply accordingly for the officers of the requesting Contracting Party. (9) An official Letter of Request, demanding a controlled delivery, over which control begins or is continued into a third State, shall be granted only if in the request is indicated that the conditions set out in paragraph 2 are also met by the third State. Article 14 of MKPS in connection to Article 15 of MKPS:	

Relevant items	Provisions	Sources used
	(5) The surveillance referred to in paragraphs 1 and 2 shall be carried out only under the following general conditions: a) The officers carrying out the surveillance must comply with the provisions of this Article and with the law of the Contracting Party in whose territory they are operating; they must obey the instructions of the competent local authorities. b) Except in the situations outlined in paragraph 2, the officers shall, during the surveillance, carry a document certifying that authorisation has been granted. c) The officers carrying out the surveillance must at all times be able to prove that they are acting in an official capacity. d) The officers carrying out the surveillance may carry their service weapons during the surveillance unless specifically otherwise decided by the requested Party; their use shall be prohibited except in cases of legitimate self-defence. e) Entry into private homes and places not accessible to the public is prohibited. f) The officers carrying out the surveillance may neither challenge nor arrest the person under surveillance. g) All operations shall be the subject of a report to the authorities of the Contracting Party in whose territory they took place; the officers carrying out the surveillance may be required to appear in person. h) The authorities of the Contracting Party from which the surveillance officers have come shall, when requested by the authorities of the Contracting Party in whose territory the surveillance took place, assist the enquiry subsequent to the operation in which they took part, including judicial proceedings, provided that the identity of the involved officer is protected. (6) The officers referred to in the previous paragraphs shall be specified in the bilateral Implementation Agreements. (7) The Contracting Parties may, by way of bilateral Implementation Agreement, extend the scope of this Article and adopt additional measures in application thereof.	
For what types of crime can the tool be used?	Article 159 (Criminal procedure code - ZKP) <i>"The arrest of a suspect and the execution of other measures provided by this Act may be temporarily postponed with a view to discovering a major criminal activity but only if, and as long as, the lives and health of third persons are not thereby endangered. Permission to postpone these measures shall upon a properly reasoned proposal by the internal affairs agency be granted by the public prosecutor with appropriate jurisdiction"</i> Mentioned only in BATPS and MKPS. However, also the provisions lists types of SOC as examples: Article 11 of BATPS "(1) At the request of the requesting Contracting Party, the requested Contracting Party may authorize controlled imports into its territory, controlled transit or controlled exports, in particular in the case of illicit trafficking in narcotic drugs, arms, explosives, counterfeit money, stolen goods and concealment and money laundering if the disclosure of end-customer and other participants or the discovery of distribution channels would otherwise be unsuccessful or substantially difficult in the opinion of the requesting Party..." Article 15 in MKPS 1) Upon Letter of Request from a Contracting Party, another Contracting Party can, in case of investigations for extraditable offences, if appropriate, permit controlled delivery on its territory, especially of transport of narcotic drugs, precursors, firearms, explosives, counterfeit currency, and items originating from a crime, or intended to be used to commit a crime, if the requesting Contracting Party explains that, without such a measure, identification of perpetrators or of distributing routes would be impossible or extremely hampered. If the content of a controlled delivery presents a particular risk for the persons involved, or a danger to the public, the requested Contracting Party has the right to ask that certain conditions to be met before granting the request or refuse the request altogether.	• ZKP (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362# • ZKP (English - not all changes and amendments are included) https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf • BATPS (Slovenian & German): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2004-02-0052/#I.%C2%A0poglavjeSplo%C5%A1ne%C2%A0dolo%C4%8Dbe
Does national law allow this tool to be used in cross border cases?	Yes	
What thresholds must be passed for the use of this tool?	Article 55 (3) of ZSKZDČEU-1: (3) A controlled delivery shall be permitted at the request of a competent authority of a Member State, or in agreement with another Member State, if criminal offences are involved which meet the conditions for issuing a European Arrest Warrant. Article 9 of ZSKZDČEU-1 (Admissibility of order execution in the Republic of Slovenia) in relation to Article 55 in ZSKZDČEU-1: (1) Surrendering a person on the basis of a warrant (i.e. European Arrest Warrant) is admissible if the warrant is issued for a criminal offence punishable in the ordering State by deprivation of liberty for a maximum period of at least one year, or for the purpose of enforcing a custodial sentence, safety measure or other measure imposed by a criminal court involving deprivation of liberty for at least four months, and if the act for which surrender is requested is also considered a criminal offence under the national penal code (double criminality).	• Cooperation Act (Slovenian): http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6513 • Cooperation Act (English): https://www.ejtn.eu/PageFiles/6533/2014%20seminars/Nicosia/SI_Legislation/Law_Cooperation_Criminal_Matters.pdf

Relevant items	Provisions	Sources used
	(2) Double criminality shall not be established if the warrant is ordered for a criminal offense for which the law of the issuing State prescribes a sentence of deprivation of liberty of at least three years as a ceiling and is one of the following criminal offenses under the law of that State: - belonging to a criminal organisation, - terrorism, - trafficking in human beings, - sexual exploitation of children and child pornography, - illicit drug trafficking, - illicit trafficking in arms, munitions and explosives, - corruption, - fraud, including that affecting the financial interests of the European Communities as defined by the Convention on the protection of the European Communities' financial interests of 26 July 1995 (OJ C 316, 27.11.1995), - money laundering, - counterfeiting money, - computer-related offenses, - offenses against the environment, space and natural resources, including illicit trafficking in endangered animal and plant species and subspecies, - facilitating the prohibited crossing of the state border and residence in the country, - murder and grievous bodily harm, - illicit trafficking in human organs and tissues, - kidnapping, unlawful deprivation of liberty and hostage-taking, - racism and xenophobia, - group robbery or armed robbery, - illicit trafficking in cultural goods, including antiques and works of art, - deception, - extortion and usury, - counterfeiting of industrial products and sale of such products, - forgery and trafficking in official documents, - counterfeiting of means of payment, - illicit trafficking in hormonal substances and other growth promoters, - illicit trafficking in nuclear and radioactive materials, - shop with stolen vehicles, - rape, - arson, - offenses within the jurisdiction of the International Criminal Court established by the Rome Statute, - hijacking of an aircraft or ship, - sabotage.	
What types of stakeholder are involved in the implementation of this tool?	According to Article 55 of ZSKZDČEU-1 the decision on controlled delivery shall fall within the competences of a district state prosecutor and controlled delivery shall be exercised by the competent Slovenian authorities (i.e. Police - <i>added by EY</i>) in a manner which ensures permanent supervision and appropriate action. According to Article 11 of BATPS the requests shall be addressed a to the Ministry of the Interior, the General Police Administration, the Criminal Police Administration in Slovenia. According to Article 10 of BITČPS the request referred from the previous paragraph must be sent: to: the Ministry of the Interior, the Police, the General Police Administration, the Criminal Police Administration.	• Cooperation Act (Slovenian): http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6513 • Cooperation Act (English): https://www.ejtn.eu/PageFiles/6533/2014%20seminars/Nicosia/SI_Legislation/Law_Cooperation_Criminal_Matters.pdf • BATPS (Slovenian & German): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2004-02-0052/#I.%C2%A0poglavjeSplo%C5%A1ne%C2%A0dolo%C4%8Dbe • BITČPS (Slovenian & Italian): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0134?sop=2007-02-0134
Which LEAs can use this tool?	Police	• Cooperation Act (Slovenian): http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6513 • Cooperation Act (English): https://www.ejtn.eu/PageFiles/6533/2014%20seminars/Nicosia/SI_Legislation/Law_Cooperation_Criminal_Matters.pdf
What are the rules to be followed for the implementation of this tool?	Rules mentioned in Slovenian legislation: Article 55 of ZSKZDČEU-1: (4) In the territory of the Republic of Slovenia, controlled delivery shall be exercised by the competent Slovenian authorities in a manner which ensures permanent supervision and appropriate action. Article 11 of BATPS: (4) Points c, d, e, h, i and j of the fifth paragraph of Article 7 of this Agreement shall apply mutatis mutandis to the execution of a controlled consignment. Article 7 (in relation to the paragraph 4. of Article 11 BATPS)	• Cooperation Act (Slovenian): http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6513 • Cooperation Act (English): https://www.ejtn.eu/PageFiles/6533/2014%20seminars/Nicosia/SI_Legislation/Law_Cooperation_Criminal_Matters.pdf • BATPS (Slovenian & German): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2004-02-0052/#I.%C2%A0poglavjeSplo%C5%A1ne%C2%A0dolo%C4%8Dbe • BHUCPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0029?sop=2007-02-0029

Relevant items	Provisions	Sources used
	(5) Covert surveillance and tracking in accordance with the first and third paragraphs of this Article is permitted only under the following conditions: c) officials carrying out covert surveillance must always be able to prove their official function; d) officials carrying out covert surveillance and surveillance may carry their service weapons during such surveillance, unless the requested Party expressly objects. The use of weapons is only allowed in the self-defence; e) entry into apartments and publicly inaccessible land is not allowed. Entry into publicly accessible working, operating and business premises is possible during their working, operating and business hours; h) the authorities of the Contracting Party from which the secret surveillance and tracking officials come shall, upon request, provide support for the subsequent investigation, including the legal proceedings of the Contracting Party in whose territory the covert surveillance and tracking took place; i) the technical means necessary to carry out covert surveillance and surveillance may be used to the extent necessary in accordance with the national law of the Contracting Party in whose territory it is carried out. The technical means used for covert surveillance and tracking must be specified in the request referred to in the first paragraph of this Article; j) the vehicles used are, in terms of exemption from traffic bans and traffic restrictions, equivalent to those of the security authorities of the Contracting Party in whose territory they are used. Signalling may be used if necessary for the purpose of conducting covert surveillance and tracking. Article 15 of MKPS (8) In the course of a controlled delivery, the provisions of Article 14, paragraph 5, sub-paragraph a) to c) and e) to h) shall apply accordingly for the officers of the requesting Contracting Party. Article 14 of MKPS in connection to Article 15 (5) The surveillance referred to in paragraphs 1 and 2 shall be carried out only under the following general conditions: a) The officers carrying out the surveillance must comply with the provisions of this Article and with the law of the Contracting Party in whose territory they are operating; they must obey the instructions of the competent local authorities. b) Except in the situations outlined in paragraph 2, the officers shall, during the surveillance, carry a document certifying that authorisation has been granted. c) The officers carrying out the surveillance must at all times be able to prove that they are acting in an official capacity. d) The officers carrying out the surveillance may carry their service weapons during the surveillance unless specifically otherwise decided by the requested Party; their use shall be prohibited except in cases of legitimate self-defence. e) Entry into private homes and places not accessible to the public is prohibited. f) The officers carrying out the surveillance may neither challenge nor arrest the person under surveillance. g) All operations shall be the subject of a report to the authorities of the Contracting Party in whose territory they took place; the officers carrying out the surveillance may be required to appear in person. h) The authorities of the Contracting Party from which the surveillance officers have come shall, when requested by the authorities of the Contracting Party in whose territory the surveillance took place, assist the enquiry subsequent to the operation in which they took part, including judicial proceedings, provided that the identity of the involved officer is protected. (6) The officers referred to in the previous paragraphs shall be specified in the bilateral Implementation Agreements. (7) The Contracting Parties may, by way of bilateral Implementation Agreement, extend the scope of this Article and adopt additional measures in application thereof. Secretariat for MKPS prepared a manual for execution of the convention: Operation Special techniques may be used provided that the use of these techniques is legal in the requested State. The requested State shall be responsible for leading and monitoring the operation in its territory and shall have the authorisation to intervene. Upon mutual agreement between the requesting and requested State, the officers of the requesting Contracting Party can continue the controlled delivery together with officers of the requested Contracting Party. 5.3.1. Emergency intervention In the event of a controlled delivery and if the competent law enforcement authorities of the requested Contracting Party cannot intervene in due time, and if continuation of the controlled delivery would present a serious risk for life or health of persons, or cause serious damage to property, or if the delivery could no longer be kept under control, the officers of the requesting Contracting Party can seize the controlled delivery. If necessary, the officers of the requesting Contracting Party can stop and apprehend persons who escort the shipment until intervention by law enforcement authorities of the requested Contracting Party.	• BITČPS (Slovenian & Italian): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0134?sop=2007-02-0134 • MKPS https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2012-02-0103/zakon-o-ratifikaciji-konvencije-o-policijskem-sodelovanju-v-jugovzhodni-evropi-mkps

Relevant items	Provisions	Sources used
	In any case the requesting Contracting Party shall inform the law enforcement authorities of the requested Contracting Party without delay. 5.3.2. Seizure of a controlled delivery If a controlled delivery has been seized, it may be handed over to the requesting Contracting Party on the basis of a letter of request. 5.3.3. Arresting of a suspect If during the operation a person was arrested and if this person is not a national of the Contracting Party in whose territory he/she was arrested, that person shall be released no later than six hours after the arrest was made, not including the hours between midnight and 9.00 a.m., unless the competent local authorities have previously received a request for that person's provisional arrest for the purposes of extradition in any form whatsoever. 5.3.4. Controlled delivery into Third States Where the controlled delivery involves more than two States, authorisation, upon a letter of request, must be obtained from the transit and destination State(s) and only if the requested State(s) guarantee(s) permanent surveillance of the shipment in a manner that enables police intervention at any time. 5.4. Annex (Draft form VIII) The Contracting Parties are invited, when necessary and appropriate, to use the draft letter of request "Cross-border Surveillance and Controlled Delivery", attached to this manual under Annex 8.8., draft form VIII.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Safeguards are for third parties (their lives and health cannot be endangered) and tool can be used only if criminal prosecution in other country is expected (this could be seen as safeguard). Article 55 of ZSKZDČEU-1 (5) Controlled delivery shall not be permitted, or its further execution shall be discontinued if: 1. or until there is a risk to people's life or health; or 2. it is likely that further supervision or action in another Member State is not ensured or will not be effective. (6) After the execution of a controlled delivery, a competent state prosecutor must establish that the conditions exist for referring criminal prosecution to the Member State in which suspects have been deprived of liberty.	- Cooperation Act (Slovenian): http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6513 - Cooperation Act (English): https://www.ejtn.eu/PageFiles/6533/2014%20seminars/Nicosia/SI_Legislation/Law_Cooperation_Criminal_Matters.pdf
What authorisation is needed for the use of this tool?	Article 55 of ZSKZDČEU-1: (2) Rendering a decision on controlled delivery shall fall within the competences of a district state prosecutor through whose area of authority the controlled delivery is envisaged to cross the state border, or from the area of whom it is dispatched, or a Specialised Office of the State Prosecutor of the Republic of Slovenia.	- Cooperation Act (Slovenian): http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6513 - Cooperation Act (English): https://www.ejtn.eu/PageFiles/6533/2014%20seminars/Nicosia/SI_Legislation/Law_Cooperation_Criminal_Matters.pdf
What ongoing supervision is required for the use of this tool?	According to Article 45 of Criminal Procedure Act the district state prosecutor directs preliminary criminal proceedings. <i>The general provision includes supervision of police activities related also to control delivery.</i> Article 55 of ZSKZDČEU-1: (4) In the territory of the Republic of Slovenia, controlled delivery shall be exercised by the competent Slovenian authorities in a manner which ensures permanent supervision and appropriate action.	- Cooperation Act (Slovenian): http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6513 - Cooperation Act (English): https://www.ejtn.eu/PageFiles/6533/2014%20seminars/Nicosia/SI_Legislation/Law_Cooperation_Criminal_Matters.pdf - ZKP (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362# - ZKP (English - not all changes and amendments are included) https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Data available on the number of times this tool has been used for SOC cases	N/A	
Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Procedure Act (ZKP), Official Gazette no. 32/12 – consolidated version, no. 47/13, 87/14, 8/16 – Constitutional Court decision, 64/16 – Constitutional Court decision, 65/16 – Constitutional Court decision, 66/17 – ORZKP153,154, 22/19, 55/20 - Constitutional Court decision, 89/20 - Constitutional Court decision, 191/20 - Constitutional Court decision and no. 200/20) Cooperation in Criminal Matters with the Member States of the European Union Act (ZSKZDČEU-1), Official Gazette of Republic of Slovenia no. 48/13, 37/15 in 22/18 Agreement between the Republic of Slovenia and the Republic of Austria on Police Cooperation (BATPS) Agreement between the Republic of Slovenia and the Republic of Hungary on cross-border co-operation of law enforcement authorities (BHUČPS) Agreement between the Republic of Slovenia and the Republic of Italy on cross-border police cooperation (BITČPS) Agreement between the Republic of Slovenia and the Republic of Croatia on Cross-border police co-operation (BHRPS) - hot pursuit is not defined (according to non-public information the hot pursuit is not allowed to Croatia since s not part of Schengen area) CONVENTION IMPLEMENTING THE SCHENGEN AGREEMENT (Convention)	- ZKP (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362# - ZKP (English - not all changes and amendments are included) https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf - Cooperation Act (Slovenian): http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6513 - Cooperation Act (English): https://www.ejtn.eu/PageFiles/6533/2014%20seminars/Nicosia/SI_Legislation/Law_Cooperation_Criminal_Matters.pdf - BATPS (Slovenian & German): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2004-02-0052/#I.%C2%A0poglavjeSplo%C5%A1ne%C2%A0dolo%C4%8Dbe - BHUČPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0029?sop=2007-02-0029 - BITČPS (Slovenian & Italian): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0134?sop=2007-02-0134

Relevant items	Provisions	Sources used
	Police Tasks And Powers Act (official Gazette of Republic of Slovenia no. 15/13, 23/15 – popr., 10/17, 46/19 – odl. US in 47/19) (ZNPPol) Police Cooperation Convention for Southeast Europe (Official Gazette of Republic of Slovenia no. 18/12) (MKPS)	• BHRPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2003-02-0014?sop=2003-02-0014 • Convention (English) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:42000A0922(02)&from=SL • ZNPPol (Slovenian) http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6314 • MKPS (English) https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2012-02-0103/zakon-o-ratifikaciji-konvencije-o-policijskem-sodelovanju-v-jugovzhodni-evropi-mkps
How is the tool defined?	Slovenia is part of the Schengen agreement consequently the Convention applies to Slovenia, including the provisions about Hot pursuits. Hot pursuits is not regulated in Cooperation in Criminal Matters with the Member States of the European Union Act, but by the bilateral agreements with the neighbouring countries. Article 9 in BATPS (1) The security authorities of a Contracting Party pursuing in their country a person who a) is caught in the commission of an offense for which extradition may be requested in the other Contracting Party, or participates in or is prosecuted for such an offense, or b) is on the run from custody or imprisonment or before any other measure of deprivation of liberty for an offense for which there is a possibility of extradition in the other Contracting Party, are authorised to continue the hot pursuit in its territory without the prior approval of the other Party if the competent authorities of the other Party could not be notified in advance due to the urgency of the matter or were not present in time to take over the hot pursuit. (2) Officials carrying out hot pursuit shall immediately contact the competent authority of the other Contracting Party, as a rule before crossing the state border. The hot pursuit shall cease as soon as the Party in whose territory the hot pursuit is to continue or is continuing so requests. At the request of the officials conducting the hot pursuit, the locally competent authorities shall, in accordance with national law, detain the pursued person in order to establish his identity or to apprehend him. (3) If no request is made to suspend the hot pursuit and the locally competent authorities cannot be involved in time, the officials conducting the hot pursuit may detain the person in accordance with the provisions of the national law of the other Contracting Party until the officials of the other Contracting Party, do not establish its identity or apprehend it. (4) The hot pursuit shall be carried out without spatial or temporal restrictions. In this case, the state border can also be crossed outside border crossings and not only during their operation. (5) The hot pursuit may be carried out only under the following conditions: a) the pursuing officers shall comply with the provisions of this Treaty and with the national law of the Contracting Party in whose territory they are operating. They shall comply with the orders of the locally competent authorities of that Contracting Party; b) hot pursuit is permitted across land, air and water borders; c) entry into dwellings and publicly inaccessible land is not allowed. Entry into publicly accessible working, operating and business premises is possible during their working, operating and business hours; d) the officers conducting the hot pursuit must be clearly identifiable, e.g. by uniform, special markings or additional devices on the vehicle. The wearing of civilian clothes while using a civilian company car without the above-mentioned markings is not permitted. Officials conducting the pursuit must always be able to prove their official function; e) officials conducting the hot pursuit may carry their service weapons during the hot pursuit. The use of weapons is only allowed in the self-defense; f) A person detained in accordance with paragraph 3 of this article may only be subjected to a security check before being brought directly to the local competent authority of the other Contracting Party. Binding and locking means may be used during the transfer. The property of that person may be temporarily seized until the arrival of the competent authorities of the other Contracting Party; g) officials carrying out hot pursuit in accordance with the provisions of paragraph 1 of this article shall, immediately after each pursuit, report to the locally competent authorities of the other Contracting Party. At their request, they are obliged to ensure their presence until all the circumstances of the hot pursuit have been clarified. This also applies to cases where the pursued person has not been detained; h) the authorities of the Contracting Party from which the hot pursuing officials come shall, upon request, provide support for the subsequent investigation, including the legal proceedings of the Contracting Party in whose territory the hot pursuit was carried out; i) the vehicles used are, in terms of exemption from traffic bans and traffic restrictions, equivalent to those of the security authorities of the Contracting Party in whose territory they are used. Signalling may be used if necessary for hot pursuit purposes; j) the technical means necessary for the hot pursuit may be used to the extent necessary in accordance with the national law of the Contracting Party in whose territory the pursuit continues.	• ZKP (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362# • ZKP (English - not all changes and amendments are included) https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf • Cooperation Act (Slovenian): http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6513 • Cooperation Act (English): https://www.ejtn.eu/PageFiles/6533/2014%20seminars/Nicosia/SI_Legislation/Law_Cooperation_Criminal_Matters.pdf • BATPS (Slovenian & German): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2004-02-0052/#I.%C2%A0poglavjeSplo%C5%A1ne%C2%A0dolo%C4%8Dbe • BHUČPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0029?sop=2007-02-0029 • BITČPS (Slovenian & Italian): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0134?sop=2007-02-0134 • BHRPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2003-02-0014?sop=2003-02-0014 • Convention (English) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:42000A0922(02)&from=SL • ZNPPol (Slovenian) http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6314 • MKPS (English) https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2012-02-0103/zakon-o-ratifikaciji-konvencije-o-policijskem-sodelovanju-v-jugovzhodni-evropi-mkps

Relevant items	Provisions	Sources used
	The competent authorities of the other Contracting Party shall be notified of the technical means used. (6) A person apprehended by officials of the competent authorities on the basis of the third paragraph of this Article may, regardless of his or her nationality, be detained for questioning. The provisions of national law shall apply mutatis mutandis. If the person is not a national of the Contracting Party in whose territory he or she was detained, he or she shall be released no later than six hours after the detention, excluding hours between midnight and nine o'clock, unless the local authority receives a request before the expiry of that period for temporary detention for extradition. Provisions of national law allowing detention or temporary detention for other reasons remain unchanged. (7) In the case of cross-border hot pursuit, the following should be informed: - in the Republic of Slovenia, the Kranj Police Administration or the Slovenj Gradec Police Administration or the Celje Police Administration or the Maribor Police Administration or the Murska Sobota Police Administration, if it falls within their local jurisdiction, - in the Republic of Austria, the Security Directorate for the Land of Burgenland or the Security Directorate for the Land of Carinthia or the Security Directorate for the Land of Styria, if it falls within their territorial jurisdiction. Those authorities shall immediately inform their national central office. Article 10 in BATPS (1) The pursuit is also admissible if the person evaded police or customs control at a distance of no more than 30 km from the state border and did not observe unambiguous signs of stopping and consequently public safety would be endangered. (2) Article 9 of this Treaty shall apply mutatis mutandis to pursuit under this Article. (3) The pursuit shall also be terminated if the competent authority of the Contracting Party in whose territory the pursuit is carried out so requests or if the continuation of the pursuit would lead to a concrete threat to the life or health of the pursued person or third parties. It must be prevented. Article 12 in BHUČPS 1. The authorised co-operating authority of the requesting Contracting Party may, without prior authorisation of the other Contracting Party, continue the pursuit in the territory of the requested Contracting Party if the person concerned committed or attempted to commit, in the territory of the requesting Contracting Party, a criminal act which serves as the basis for issuing the European arrest warrant and: a) was caught in the act or b) escaped from detention, provisional custody or while serving a sentence involving deprivation of liberty and if the delay caused by notifying the authorised co-operating authority of the requested Contracting Party would render the arrest of the perpetrator substantially more difficult or severely jeopardise the interests of crime suppression and it is probable that the authorised co-operating authority of the requested Contracting Party would not be able to take over the pursuit in time. 2. In the cases referred to in Paragraph (1), the competent authorised co-operating authority of the requested Contracting Party shall be notified as soon as possible, but not later than at the time of crossing the state border. 3. The competent authorised co-operating authorities under Paragraph (2) shall be: a) for the Slovenian Contracting Party: - the Murska Sobota Police Directorate; b) for the Hungarian Contracting Party, depending on the place of crossing the state border: - Zala County Police Directorate, - Vas County Police Directorate. 4. The hot pursuit shall cease immediately if so required by the authorised co-operating authority of the requested Contracting Party. 5. If the pursuing officer of the requesting Contracting Party so requests, the authorised co-operating authority of the requested Contracting Party shall challenge the pursued person in order to establish the person's identity or to make an arrest. 6. If no request to cease the hot pursuit is made and if the authorised co-operating authority is unable to intervene quickly enough, the pursuing officers of the requesting Contracting Party may detain the person pursued on the spot. The competent authorised co-operating authority of the requested Contracting Party shall be immediately notified of this action. 7. The pursuit may be carried out in the entire territory of the Contracting Parties without limits in time. 8. The pursuit may be carried out according to the following conditions: a) the pursuing officer must comply with the provisions of this Agreement and with the laws and regulations of the Contracting Party in whose territory he is operating; b) the pursuit may be carried out exclusively on land;	

Relevant items	Provisions	Sources used
	c) the pursuing officer may not enter private homes or premises, but may enter work, plant and business premises open to the public during working hours; d) the pursuing officers must at all times be able to prove that they are acting in an official capacity; e) in using vehicles in the course of pursuit, the traffic rules of the requested Contracting Party shall be observed. A vehicle must be identifiable by means of an accessory fitted to the vehicle; f) the pursuing officer shall be identifiable unambiguously by his uniform or accessories fitted to the vehicle; g) objects in possession of the arrested individual shall preferably be stored in a safe place until the arrival of the authorised co-operating authorities; h) if technical instruments are required for the conduct of hot pursuit, they may be used if this is enabled under the laws and regulations of the requested Contracting Party; i) after completion of the pursuit, the pursuing officers shall report on their mission to the competent authorised co-operating authority or central contact point of the requested Contracting Party. At the request of those authorities, they shall remain at their disposal until the circumstances surrounding their action have been sufficiently clarified. This condition shall apply even where the hot pursuit has not resulted in the arrest of the person pursued. 9. The person arrested in the course of the pursuit shall be questioned by the authorised co-operating authority of the requested Contracting Party. The person's freedom may be restricted in accordance with the laws and regulations of the requested Contracting Party. 10. The central contact point of the Contracting Party shall be notified of the pursuit. Article 8 in BITCPS (1) The security authorities of a Contracting Party pursuing in their country a person, who: a) is caught or prosecuted for an offense or participation in an offense for which extradition may be requested in the other Contracting Party, b) has escaped from custody or imprisonment or is fleeing from other measures of deprivation of liberty taken for the offenses for which extradition is admissible, are authorised to continue the hot pursuit in its territory without the prior approval of the other Contracting Party if the competent authorities of the other Contracting Party have not been able to notified in advance due to the urgency of the matter or if the hot pursuit has not been hand over. (2) The pursuing officials shall immediately contact the competent authority of the other Contracting Party, as a general rule before crossing the national border. The hot pursuit shall be terminated as soon as requested by the Party in whose territory the hot pursuit is to continue or is continuing. At the request of the officials conducting the hot pursuit, the locally competent authorities shall, in accordance with national law, detain the pursued person in order to establish his identity or deprive him of his liberty. (3) In the absence of a request for the cessation of the hot pursuit and in the absence of timely involvement of the locally competent authorities, the officials conducting the hot pursuit may detain the person in accordance with the domestic law of the other Party until the officials of the other Party are notified, establish her identity or do not apprehend her. (4) The hot pursuit shall be carried out without spatial or temporal limitation. In this case, the state border can also be crossed outside border crossings and outside their operating hours. (5) The hot pursuit may be carried out only under the following conditions: a) officials must comply with this Agreement and the national law of the Contracting Party in whose territory they are operating. They shall comply with the orders of the locally competent authorities of that Contracting Party; b) hot pursuit is permitted across land, air and water borders; c) entry into dwellings and places not accessible to the public is not permitted. Entry into publicly accessible working, operating and business premises is possible during their working, operating or business hours; d) officials must be clearly identifiable by their uniform or special official markings or additional devices on the vehicle. The wearing of civilian clothes while using a civilian company car without the aforementioned official markings is not permitted. Officials must always be able to prove their position; e) officials may carry their service weapons during the hot pursuit. The use of weapons is only allowed in the self-defense; f) a person detained in accordance with paragraph 3 may only be subjected to a security check before being brought directly to the competent authority of the other Contracting Party. Binding and locking means may be used during the transfer. Items carried by that person may be suspended until the arrival of the competent authorities of the other Contracting Party; g) After each hot pursuit, officials shall report immediately to and report to the local competent authorities of the other Contracting Party. At their request, they must ensure their presence until all the circumstances of the hot pursuit have been clarified. This also applies to cases where the pursued person has not been arrested;	

Relevant items	Provisions	Sources used
	h) the authorities of the Contracting Party from which the officials conducting the hot pursuit come shall, upon request, provide assistance in continuing the investigation; i) the vehicles used shall be treated in the same way as the vehicles of the security authorities of the Contracting Party in whose territory they are used in terms of exemption from traffic bans and traffic restrictions. Signalling may be used if necessary to carry out the hot pursuit; j) the technical means necessary to carry out the hot pursuit may be used to the extent necessary in accordance with the domestic law of the Contracting Party in whose territory the hot pursuit continues. The competent authorities of the other Contracting Party shall be notified of the technical means used. (6) A person apprehended by officials of the competent authorities pursuant to paragraph 3 may be detained for questioning. In doing so, domestic law shall apply. (7) In the case of cross-border hot pursuit, the following shall be informed: - in the Republic of Slovenia: Center for Police Cooperation Vrata - Megvarje or the Koper Police Administration or the Nova Gorica Police Administration or the Kranj Police Administration, if it falls within their local jurisdiction; - in the Italian Republic: the Center for Police Cooperation Vrata - Megvarje and the Ministry of the Interior, the Public Security Administration, the Central Directorate of the Criminal Police - the International Police Cooperation Service. Article 9 in BITCPS (1) The pursuit shall also be permitted if the person evaded police control at a maximum distance of 30 km from the state border and did not comply with the intended stop signs and could therefore endanger public safety. (2) Article 8 shall apply mutatis mutandis to the pursuit referred to in this Article. (3) The pursuit shall be terminated if the competent authority of the Contracting Party in whose territory the pursuit takes place so requests, or if the continuation of the pursuit would endanger the life and health of the pursued person or third parties. Article 111 in ZNPPol Police officers are allowed to pursue and capture a vessel that does not stop at police signals. In statutory cases where the conditions for detention or detention have been met, the vessel, crew members in other persons on board may be taken to a designated place or to the competent authority. Article 13 from MKPS (1) Officers of one of the Contracting Parties who are pursuing in their country an individual caught in the act of committing or participating in a criminal offence shall be allowed, subject to bilateral Implementation Agreements concluded in accordance with Article 34 paragraph 1 of this Convention, to continue pursuit in the territory of another Contracting Party without the latter's prior authorisation, where given the particular urgency of the situation, it is not possible to notify the law enforcement authorities of the other Contracting Party by one of the means provided for in Article 24 of the Convention prior to entry into that territory or where these authorities are unable to reach the scene in time to take over the pursuit. The same shall apply where the person being pursued has escaped from provisional custody or while serving a sentence involving deprivation of liberty. The pursuing officers shall, not later than when they cross the border, contact the law enforcement authorities of the Contracting Party in whose territory the hot pursuit is to take place. The hot pursuit will cease as soon as the Contracting Party in whose territory the pursuit is taking place so requests. At the request of the pursuing officers, the competent local authorities shall challenge the pursued person in order to establish the person's identity or to make an arrest. (2) The bilateral Implementation agreements as referred to in paragraph 1 of this Article shall define the criminal offences for which the hot pursuit will be applicable either by way of an exhaustive list or by extending it to all extraditable criminal offences. (3) Hot pursuit shall be carried out in accordance with one of the following procedures, defined by the bilateral Implementation Agreements as referred to in paragraph 1 and 2 of this Article: a) The pursuing officers shall not have the right to apprehend the pursued person; b) If no request to cease the hot pursuit is made and if the competent local authorities are unable to intervene quickly enough, the pursuing officers may detain the person pursued until the officers of the Contracting Party in whose territory the pursuit is taking place, who must be informed immediately, are able to establish the person's identity or make an arrest. (4) Hot pursuit shall be carried out in accordance with paragraphs 1 and 3 and in one of the following ways as defined by the bilateral Implementation Agreements as referred to in paragraph 1 and 2 of this Article: a) in an area or during a period as from the crossing of the border, to be established in the bilateral Implementation Agreement; b) without limit in space or time. (5) Hot pursuit shall be carried out only under the following general conditions:	

Relevant items	Provisions	Sources used
	a) The pursuing officers must comply with the provisions of this Article and with the law of the Contracting Party in whose territory they are operating; they must obey the instructions issued by the competent local authorities. b) Pursuit shall be solely over land and blue borders. c) Entry into private homes and places not accessible to the public is prohibited. d) The pursuing officers shall be easily recognisable, either by their uniform, by means of an armband or by accessories fitted to their vehicles; the use of civilian clothes combined with the use of unmarked vehicles without the aforementioned identification is prohibited; the pursuing officers must at all times be able to prove that they are acting in an official capacity. e) The pursuing officers may carry their service weapons; their use shall be prohibited except in cases of legitimate self-defence. f) Once the pursued person has been apprehended as provided for in paragraph 3(b), for the purpose of being brought before the competent local authorities that person may only be subjected to a security search; handcuffs may be used during the transfer; objects carried by the pursued person may be seized. g) After each operation referred to in paragraphs 1, 3 and 4, the pursuing officers shall appear before the competent local authorities of the Contracting Party in whose territory they were operating and shall report on their mission; at the request of those authorities, they shall remain at their disposal until the circumstances surrounding their action have been sufficiently clarified; this condition shall apply even where the hot pursuit has not resulted in the arrest of the person pursued. h) The authorities of the Contracting Party from which the pursuing officers have come shall, when requested by the authorities of the Contracting Party in whose territory the hot pursuit took place, shall assist the enquiry subsequent to the operation in which they took part, including judicial proceedings, providing that the identity of the involved pursuing officer is protected. (6) A person who, following the action provided for in paragraph 3, has been arrested by the competent local authorities may, whatever that person's citizenship, be held for questioning. The relevant rules of national law shall apply mutatis mutandis. If the person is not a national of the Contracting Party in whose territory the person was arrested, that person shall be released no later than six hours after the arrest was made, not including the hours between midnight and 9.00 a.m., unless the competent local authorities have previously received a request for that person's provisional arrest for the purposes of extradition in any form whatsoever. (7) The officers referred to in the previous paragraphs shall be specified in the bilateral Implementation Agreements. (8) The Contracting Parties may, on a bilateral basis, extend the scope of paragraph 1 and adopt additional provisions in implementation of this Article.	
For what types of crime can the tool be used?	Not defined in Criminal Procedure Code: - Cross crime areas	• MKPS (English) https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2012-02-0103/zakon-o-ratifikaciji-konvencije-o-policijskem-sodelovanju-v-jugovzhodni-evropi-mkps
Does national law allow this tool to be used in cross border cases?	Yes (see provisions of bilateral agreements)	•
What thresholds must be passed for the use of this tool?	Article 12 in BHUČPS: 1. The authorised co-operating authority of the requesting Contracting Party may, without prior authorisation of the other Contracting Party, continue the hot pursuit in the territory of the requested Contracting Party if the person concerned committed or attempted to commit, in the territory of the requesting Contracting Party, a criminal act which serves as the basis for issuing the European arrest warrant and: a) was caught in the act or b) escaped from detention, provisional custody or while serving a sentence involving deprivation of liberty and if the delay caused by notifying the authorised co-operating authority of the requested Contracting Party would render the arrest of the perpetrator substantially more difficult or severely jeopardise the interests of crime suppression and it is probable that the authorised co-operating authority of the requested Contracting Party would not be able to take over the pursuit in time. For conditions that have to be met for issuing the European arrest warrant see Article 9 of ZSKZDČEU-1 (Admissibility of order execution in the Republic of Slovenia) above. Article 9 in BATPS (1) The security authorities of a Contracting Party pursuing in their country a person who a) is caught in the commission of an offense for which extradition may be requested in the other Contracting Party, or participates in or is prosecuted for such an offense, or b) is on the run from custody or imprisonment or before any other measure of deprivation of liberty for an offense for which there is a possibility of extradition in the other Contracting Party, are authorised to continue the hot pursuit in its territory without the prior approval of the other Party if the competent authorities of the other Party could not be notified in advance due to the urgency of the matter or were not present in time to take over the hot pursuit.	• Cooperation Act (Slovenian): http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6513 • Cooperation Act (English): https://www.ejtn.eu/PageFiles/6533/2014%20seminars/Nicosia/SI_Legislation/Law_Cooperation_Criminal_Matters.pdf • BATPS (Slovenian & German): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2004-02-0052/#I.%C2%A0poglavjeSplo%C5%A1ne%C2%A0dolo%C4%8Dbe • BHUCPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0029?sop=2007-02-0029 • BITČPS (Slovenian & Italian): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0134?sop=2007-02-0134 • BHRPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2003-02-0014?sop=2003-02-0014 •

Relevant items	Provisions	Sources used
	Article 8 in BITČPS (1) The security authorities of a Contracting Party pursuing in their country a person, who: a) is caught or prosecuted for an offense or participation in an offense for which extradition may be requested in the other Contracting Party, b) has escaped from custody or imprisonment or is fleeing from other measures of deprivation of liberty taken for the offenses for which extradition is admissible, are authorised to continue the hot pursuit in its territory without the prior approval of the other Contracting Party if the competent authorities of the other Contracting Party have not been able to notified in advance due to the urgency of the matter or if the hot pursuit has not been hand over.	
What types of stakeholder are involved in the implementation of this tool?	In all cases hot pursuit is performed by the police. Bilateral agreements define point of contact for each agreement. (See below) Article 9 in BATPS Stakeholders: - The security authorities conducting the Hot pursuit; - Kranj Police Administration or the Slovenj Gradec Police Administration or the Celje Police Administration or the Maribor Police Administration or the Murska Sobota Police Administration, if it falls within their local jurisdiction need to be informed in Slovenia. The Security Directorate for the Land of Burgenland or the Security Directorate for the Land of Carinthia or the Security Directorate for the Land of Styria, if it falls within their territorial jurisdiction need to be informed in Austria. Article 1 in BATPS in connection to Article 9 in BATPS (3) The security authorities under this Treaty are: in the Republic of Slovenia, the Ministry of the Interior, the General Police Administration, as the national central service with its internal organisational units and regional organisational units of the police (hereinafter: police administrations) within its competences, in the Republic of Austria, the Federal Minister of the Interior as the national central service, the security directorates, the federal police directorates and, outside the area of territorial competence of the federal police directorates, the district administrative bodies. Article 12 in BHUČPS Stakeholders: (3)Murska Sobota (Slovenia), Zala (Hungary) and Vas (Hungary) Police Department can conduct the Hot pursuit. (10) The central contact point of the Contracting Party shall be notified of the Hot pursuit. Article 2 in BHUČPS in connection to Article 12 in BHUČPS 2. The central contact points for the implementation of this Agreement shall be as follows: a) for the Slovenian Contracting Party: - Ministry of the Interior, Police, General Police Directorate; b) for the Hungarian Contracting Party: - National Police Headquarters International Law Enforcement Co-operation Center. Article 8 in BITČPS Stakeholders: The security authorities conducting the Hot pursuit. (7) In the case of cross-border pursuit, the following shall be informed: - in the Republic of Slovenia: Center for Police Cooperation Vrata - Megvarje or the Koper Police Administration or the Nova Gorica Police Administration or the Kranj Police Administration, if it falls within their local jurisdiction; - in the Italian Republic: the Center for Police Cooperation Vrata - Megvarje and the Ministry of the Interior, the Public Security Administration, the Central Directorate of Criminal Police - the International Police Cooperation Service. Article 1 in BITČPS in connection to Article 8 3. The security authorities under this Agreement are: in the Republic of Slovenia: the Ministry of the Interior, the Police, the General Police Administration as a national central body with its internal organisational units and regional police organisational units (hereinafter referred to as the Police Administration) within their competences; in the Italian Republic: the Ministry of the Interior, the Public Security Administration as the national central authority and the regional offices within their competences. Article 13 in MKPS Stakeholders: - Officers of one of the Contracting Parties who are conducting the Hot pursuit. - The law enforcement authorities of the Contracting Party in whose territory the hot pursuit is to take place need to be informed	• BATPS (Slovenian & German): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2004-02-0052/#I.%C2%A0poglavjeSplo%C5%A1ne%C2%A0dolo%C4%8Dbe • BHUCPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0029?sop=2007-02-0029 • BITČPS (Slovenian & Italian): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0134?sop=2007-02-0134 • BHRPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2003-02-0014?sop=2003-02-0014 • MKPS (English) https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2012-02-0103/zakon-o-ratifikaciji-konvencije-o-policijskem-sodelovanju-v-jugovzhodni-evropi-mkps
Which LEAs can use this tool?	Police	

Relevant items	Provisions	Sources used
What are the rules to be followed for the implementation of this tool?	Article 9 in BATPS: (5) The hot pursuit may be carried out only under the following conditions: a) the pursuing officers shall comply with the provisions of this Treaty and with the national law of the Contracting Party in whose territory they are operating. They shall comply with the orders of the locally competent authorities of that Contracting Party; b) hot pursuit is permitted across land, air and water borders; c) entry into dwellings and publicly inaccessible land is not allowed. Entry into publicly accessible working, operating and business premises is possible during their working, operating and business hours; d) the officers conducting the hot pursuit must be clearly identifiable, e.g. by uniform, special markings or additional devices on the vehicle. The wearing of civilian clothes while using a civilian company car without the above-mentioned markings is not permitted. Officials conducting the pursuit must always be able to prove their official function; e) officials conducting the hot pursuit may carry their service weapons during the hot pursuit. The use of weapons is only allowed in the self-defense; f) A person detained in accordance with paragraph 3 of this article may only be subjected to a security check before being brought directly to the local competent authority of the other Contracting Party. Binding and locking means may be used during the transfer. The property of that person may be temporarily seized until the arrival of the competent authorities of the other Contracting Party; g) officials carrying out hot pursuit in accordance with the provisions of paragraph 1 of this article shall, immediately after each pursuit, report to the locally competent authorities of the other Contracting Party. At their request, they are obliged to ensure their presence until all the circumstances of the hot pursuit have been clarified. This also applies to cases where the pursued person has not been detained; h) the authorities of the Contracting Party from which the hot pursuing officials come shall, upon request, provide support for the subsequent investigation, including the legal proceedings of the Contracting Party in whose territory the hot pursuit was carried out; i) the vehicles used are, in terms of exemption from traffic bans and traffic restrictions, equivalent to those of the security authorities of the Contracting Party in whose territory they are used. Signalling may be used if necessary for hot pursuit purposes; j) the technical means necessary for the hot pursuit may be used to the extent necessary in accordance with the national law of the Contracting Party in whose territory the pursuit continues. The competent authorities of the other Contracting Party shall be notified of the technical means used. Article 12 in BHUČPS 8. The pursuit may be carried out according to the following conditions: a) the pursuing officer must comply with the provisions of this Agreement and with the laws and regulations of the Contracting Party in whose territory he is operating; b) the pursuit may be carried out exclusively on land; c) the pursuing officer may not enter private homes or premises, but may enter work, plant and business premises open to the public during working hours; d) the pursuing officers must at all times be able to prove that they are acting in an official capacity; e) in using vehicles in the course of pursuit, the traffic rules of the requested Contracting Party shall be observed. A vehicle must be identifiable by means of an accessory fitted to the vehicle; f) the pursuing officer shall be identifiable unambiguously by his uniform or accessories fitted to the vehicle; g) objects in possession of the arrested individual shall preferably be stored in a safe place until the arrival of the authorised co-operating authorities; h) if technical instruments are required for the conduct of hot pursuit, they may be used if this is enabled under the laws and regulations of the requested Contracting Party; i) after completion of the pursuit, the pursuing officers shall report on their mission to the competent authorised co-operating authority or central contact point of the requested Contracting Party. At the request of those authorities, they shall remain at their disposal until the circumstances surrounding their action have been sufficiently clarified. This condition shall apply even where the hot pursuit has not resulted in the arrest of the person pursued. Article 8 in BITČPS (5) The hot pursuit may be carried out only under the following conditions: a) officials must comply with this Agreement and the national law of the Contracting Party in whose territory they are operating. They shall comply with the orders of the locally competent authorities of that Contracting Party; b) hot pursuit is permitted across land, air and water borders;	- BATPS (Slovenian & German): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2004-02-0052/#I.%C2%A0poglavjeSplo%C5%A1ne%C2%A0dolo%C4%8Dbe - BHUČPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0029?sop=2007-02-0029 - BITČPS (Slovenian & Italian): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0134?sop=2007-02-0134 - BHRPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2003-02-0014?sop=2003-02-0014 - MKPS (English) https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2012-02-0103/zakon-o-ratifikaciji-konvencije-o-policijskem-sodelovanju-v-jugovzhodni-evropi-mkps

Relevant items	Provisions	Sources used
	c) entry into dwellings and places not accessible to the public is not permitted. Entry into publicly accessible working, operating and business premises is possible during their working, operating or business hours; d) officials must be clearly identifiable by their uniform or special official markings or additional devices on the vehicle. The wearing of civilian clothes while using a civilian company car without the aforementioned official markings is not permitted. Officials must always be able to prove their position; e) officials may carry their service weapons during the hot pursuit. The use of weapons is only allowed in the self-defense; f) a person detained in accordance with paragraph 3 may only be subjected to a security check before being brought directly to the competent authority of the other Contracting Party. Binding and locking means may be used during the transfer. Items carried by that person may be suspended until the arrival of the competent authorities of the other Contracting Party; g) After each hot pursuit, officials shall report immediately to and report to the local competent authorities of the other Contracting Party. At their request, they must ensure their presence until all the circumstances of the hot pursuit have been clarified. This also applies to cases where the pursued person has not been arrested; h) the authorities of the Contracting Party from which the officials conducting the hot pursuit come shall, upon request, provide assistance in continuing the investigation; i) the vehicles used shall be treated in the same way as the vehicles of the security authorities of the Contracting Party in whose territory they are used in terms of exemption from traffic bans and traffic restrictions. Signalling may be used if necessary to carry out the hot pursuit; j) the technical means necessary to carry out the hot pursuit may be used to the extent necessary in accordance with the domestic law of the Contracting Party in whose territory the hot pursuit continues. The competent authorities of the other Contracting Party shall be notified of the technical means used. Article 13 in MKPS (5) Hot pursuit shall be carried out only under the following general conditions: a) The pursuing officers must comply with the provisions of this Article and with the law of the Contracting Party in whose territory they are operating; they must obey the instructions issued by the competent local authorities. b) Pursuit shall be solely over land and blue borders. c) Entry into private homes and places not accessible to the public is prohibited. d) The pursuing officers shall be easily recognisable, either by their uniform, by means of an armband or by accessories fitted to their vehicles; the use of civilian clothes combined with the use of unmarked vehicles without the aforementioned identification is prohibited; the pursuing officers must at all times be able to prove that they are acting in an official capacity. e) The pursuing officers may carry their service weapons; their use shall be prohibited except in cases of legitimate self-defence. f) Once the pursued person has been apprehended as provided for in paragraph 3(b), for the purpose of being brought before the competent local authorities that person may only be subjected to a security search; handcuffs may be used during the transfer; objects carried by the pursued person may be seized. g) After each operation referred to in paragraphs 1, 3 and 4, the pursuing officers shall appear before the competent local authorities of the Contracting Party in whose territory they were operating and shall report on their mission; at the request of those authorities, they shall remain at their disposal until the circumstances surrounding their action have been sufficiently clarified; this condition shall apply even where the hot pursuit has not resulted in the arrest of the person pursued. h) The authorities of the Contracting Party from which the pursuing officers have come shall, when requested by the authorities of the Contracting Party in whose territory the hot pursuit took place, shall assist the enquiry subsequent to the operation in which they took part, including judicial proceedings, providing that the identity of the involved pursuing officer is protected. According to the Manual execution of MKPS includes: Conditions - Hot pursuit requires that it has not been possible to advise the requested authorities in advance owing to particular urgency or the authorities have been informed but have not been able to take over the pursuit in time themselves. - The pursuing officer consults the authorities of the requested State at latest upon crossing the border. - The pursuit ceases at the first request of the requested State. - Reference to a national fact sheet must be made to set out the different legal situations and restrictions set by each State. - Hot pursuit shall be carried out in accordance with the bilateral agreement in an area... - Hot pursuit shall be carried out without limit in space or time. - Only officers from the designated authorities may exercise the power of pursuit.	

Relevant items	Provisions	Sources used
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Basic safeguards in provisions of bilateral and multilateral agreements (see above) Entry in private homes and premises is not allowed Use of weapon is limited to self-defence The way person is detained is regulated by the provisions of the agreements	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Police officer in hot pursuit has to inform local police administration (i.e. Operational-communication center) which informs counter party in the other country. No special authorisation is required.	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Procedure Act (ZKP), Official Gazette no. 32/12 – consolidated version, no. 47/13, 87/14, 8/16 – Constitutional Court decision, 64/16 – Constitutional Court decision, 65/16 – Constitutional Court decision, 66/17 – ORZKP153,154, 22/19, 55/20 - Constitutional Witness Protection Act (Official Gazette no. 81/06, 117/06 – ZDoh-2, 110/07 in 30/18) (ZZPrič) Agreement between the Republic of Slovenia and the Republic of Hungary on cross-border co-operation of law enforcement authorities (BHUČPS) Police Cooperation Convention for Southeast Europe (Official Gazette of Republic of Slovenia no. 18/12) (MKPS)	• ZKP (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362# • ZKP (English - not all changes and amendments are included) https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf • ZZPrič (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4265 • https://www.gov.si/assets/ministrstva/MZZ/Dokumenti/multilateralala/mednarodno-pravo/depozitarstvo/Sporazum-o-sodelovanju-pri-zasciti-pric.pdf • MKPS (English) https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2012-02-0103/zakon-o-ratifikaciji-konvencije-o-policijskem-sodelovanju-v-jugovzhodni-evropi-mkps
How is the tool defined?	Witness protection is considered as one of the general police tasks according to the Article 4 of the Police Tasks and Powers Act (ZNNPol), namely "protection of life, personal safety and property of people". Witness is according to the Article 234 of the Criminal Procedure Act (ZZPrič) defined as (1) Persons likely to give some information about the criminal offence, the perpetrator and other material circumstances shall be summoned as witnesses. Individuals covered by the Witness protection Act individuals are endangered witnesses and their close relatives (Article 3): a) an endangered person is an endangered witness or other endangered person; b) an endangered witness is a witness whose inclusion in the protection program is justified due to the circumstances specified in this Act and the Act governing criminal proceedings; c) the other endangered person is a close relative of the witness (items 1 to 3 of the first paragraph of Article 236 of the Criminal Procedure Act) or another person who is endangered due to his / her relationship with the witness; Witness protection program is defined (Article 3) as program which includes <i>measures and actions proposed, organised or implemented by the Unit for Protection of Endangered Persons, the Administration for the Execution of Criminal Sanctions, the Administration of the Prison Enforcement Institution, the Penitentiary Institution juvenile imprisonment or an institution for the enforcement of educational measures</i>. The Unit for the Protection of Endangered Persons is an organisational unit of the Police established for proposing, organizing and implementing measures and tasks under this Act. The Commission for the Protection of Endangered Persons is the body responsible for deciding on the inclusion and termination of the implementation of the protection program and for other actions determined by this Act. The Witness Protection Act includes a special acritical on International exchange (Article 27) explained below: (1) International exchange shall include the exchange of protected persons for whom the competent authority has determined a measure for the relocation of a person and the exchange of personal data in order to ensure personal security. It is carried out with the parties to international treaties, which also determine the international exchange and protection of endangered persons and bind the Republic of Slovenia. (2) The transfer of a protected person outside the territory of the Republic of Slovenia or to the territory of the Republic of Slovenia shall be carried out on the basis of a written agreement between the unit and the body of the Contracting Party referred to in the preceding paragraph. All issues related to the measures in the protection program shall be settled by written agreement. The competent witness protection authority of the requesting Contracting Party shall	• ZKP (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362# • ZKP (English - not all changes and amendments are included) https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf • ZZPrič (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4265 • Agreement (English) - https://www.gov.si/assets/ministrstva/MZZ/Dokumenti/multilateralala/mednarodno-pravo/depozitarstvo/Sporazum-o-sodelovanju-pri-zasciti-pric.pdf • MKPS (English) https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2012-02-0103/zakon-o-ratifikaciji-konvencije-o-policijskem-sodelovanju-v-jugovzhodni-evropi-mkps • ZNPPol (Slovenian) http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6314

Relevant items	Provisions	Sources used
	provide the competent witness protection authority of the Contracting Party to whose territory the protected person is to be relocated with the following personal data of the protected person: - Personal name, - the identity number of the citizen or birth data (day, month, year), country and place of birth, gender, or in the case of an alien, another general identification number assigned to him by the country of citizenship or the type and number of the travel document, - tax number, - address of permanent or temporary residence, - citizenship, - health information strictly necessary for the safe and effective implementation of the protection program, - physical characteristics (tattoos, disability), - pre-conviction, - information on open criminal proceedings against the person, - education and work experience, - membership in clubs, associations and a range of possible hobbies. (3) The competent authority for the protection of witnesses of a Contracting Party may also process data on nationality and religion, if they have been lawfully provided to it, or obtain them itself on the basis of the express personal written consent of the protected person. The obtained data are further processed for the needs of international exchange. (4) Before concluding the agreement referred to in the preceding paragraph, the unit shall notify the commission of the request of the competent authority of the Contracting Party referred to in the first paragraph of this Article for the transfer of the protected person to the territory of the Republic of Slovenia. The notification or proposal must be accompanied by an assessment of the possibility of successful implementation of the international exchange, in particular regarding the interest of the Republic of Slovenia in participating in the international exchange, ensuring personal security and the possibility of staying a protected person. The Commission shall take a decision deciding on the exchange within eight days of receipt of the notification or proposal. (5) A proposal for the transfer of a protected person outside the territory of the Republic of Slovenia shall be submitted by the unit to the commission only in accordance with the previous paragraph if the international exchange measure is not specified in the commission decision on inclusion in the protection program. (6) Cooperation between the bodies responsible for the implementation of the program for the protection of endangered persons shall take place directly. Slovenia is also party to the Agreement on the cooperation in the area of witness protection signed by the Republic of Austria, the Republic of Bulgaria, the Republic of Croatia, the Czech Republic, Hungary, Romania, Slovak Republic and the Republic of Poland on 11th Oct. 2012. According to the paragraph 2. of the Article 2. the cooperation shall, in particular include the relocation and protection of persons, exchange of information, administrative, technical and logistical support and training the staff of witness protection. The protected person to be relocated must have been placed under the national protection programme of the requesting Contracting Party, or, in case of urgent need, it must be presumable that the person will be taken into the national protection programme. Article 10 in MKPS (1) The law enforcement authorities of the Contracting Parties designated for the witness protection shall directly cooperate in the area of witness protection programmes. (2) The cooperation shall, in particular, include the exchange of information, assistance as regards logistics, and taking over of persons to be protected. (3) An Agreement will be signed for each particular case of taking over of persons to be protected, in order for mutual rights and obligations to be regulated. (4) The person to be protected must have been placed under the witness protection programme of the requesting Contracting Party. The person to be protected will not be included in the witness protection programme of the requested Contracting Party. When taking supportive measures in connection with the protection of these persons the national legislation of the requested Contracting Party shall apply accordingly. (5) In principle the requesting Contracting Party shall bear the costs of living for the persons to be protected. The requested Contracting Party shall bear the expenses for personnel and material resources for the protection of these persons. (6) For serious reasons and after having duly notified the requesting Contracting Party, the requested Contracting Party can cease the supportive measures. In this case, the requesting Contracting Party shall retake the person concerned. Article 15 in BHUČPS 1. In the course of criminal proceedings, the Contracting Parties may request via their authorised co-operating authorities that witnesses, victims and suspects and, in view of them, other persons under protection (hereinafter the persons concerned) be transferred from the territory of one	

Relevant items	Provisions	Sources used
	Contracting Party to the territory of another Contracting Party and that they be granted protection thereafter. This procedure must not obstruct the criminal proceedings in the territories of the Contracting Parties. 2. In addition to the data specified in Article 4 (1) of this Agreement, the request for handing over or taking over protection shall include: a) request for confidentiality; b) the status of the persons concerned in the criminal proceedings; c) information concerning the threat to the person and its severity; d) the reasons for moving the person concerned to the territory of the requested Contracting Party; e) the recommended form and level of protection; f) the necessary duration of stay in the territory of the requested Contracting Party and the possibility of extension. 3. After the request has been approved, the authorities in charge of providing protection shall directly agree on the handing over and taking over protection, its mode and duration and ways of maintaining contact. The documents required for performing protection shall constitute an annex to this arrangement. 4. The costs of transfer and social insurance shall be covered by the requesting Contracting Party. The requested Contracting Party shall cover the cost of salaries of the personnel protecting the persons concerned. 5. The person concerned may only benefit from the forms of protection that are provided for by the national laws and regulations on witness protection of the requested Contracting Party. 6. If after the transfer the protection can no longer be guaranteed, or cannot be guaranteed at all, the authority of the requested Contracting Party in charge of carrying out protection shall immediately inform its counterpart at the requesting Contracting Party. 7. The person concerned shall comply with the laws and regulations of the requested Contracting Party. If the person concerned violates the laws and regulations of the requested Contracting Party or fails to respect the rules of behaviour determined specifically for him, the authority of the requested Contracting Party in charge of protection shall immediately inform its counterpart at the requesting Contracting Party. 8. In the event of an act of the person concerned that would unjustifiably and severely jeopardise the staff members of the requested Contracting Party performing protection, this authority of the requested Contracting Party shall immediately initiate the return of the person concerned and its counterpart at the requesting Contracting Party shall comply with this initiative. 9. The competent authorised co-operating authorities for the implementation of this Article shall be: a) for the Slovenian Contracting Party: – Ministry of the Interior, Police, General Police Directorate; b) for the Hungarian Contracting Party: – National Police Headquarters.	
For what types of crime can the tool be used?	Cross crime areas, no limitations on types of SOC.	
Does national law allow this tool to be used in cross border cases?	Yes, Article 27 of the Witness Protection Act (see above)	
What thresholds must be passed for the use of this tool?	No limitations on types of crime, however the following must be met: Article 10 in ZZPrič: (1) For the protection of protected persons by law, the following conditions must be met: 1. that pre-trial or criminal proceedings are pending for a criminal offense in respect of which, in accordance with the provisions of the law governing criminal proceedings, covert investigative measures may be ordered by a court decision; 2. that the witness knows how to tell about the crime from the previous points, the perpetrator or other important environment; 3. that the offense cannot be investigated or proven or that the offenses cannot be further enforced, prevented without the participation of this story in pre-trial or criminal proceedings; 4. that the participation of the stories poses a serious danger to her life or the body or the lives of other physical persons; 5. not to take the risk of cooperating with agricultural groups without implementing emergency safeguards or protecting programs under the law in 6. that, on the basis of the assessment of the unit, the possibility of successful implementation of the protection program has been determined.	ZZPrič (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4265
What types of stakeholder are involved in the implementation of this tool?	The Unit for the Protection of Endangered Persons - is an organisational unit of the Police established for proposing, organizing and implementing measures and tasks under Witness protection Act.	ZZPrič (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4265

Relevant items	Provisions	Sources used
	The Commission for the Protection of Endangered Persons - is the body responsible for deciding on the inclusion and termination of the implementation of the protection program and for other acts determined by Witness protection Act. Article 7 of ZZPrič (1) The Commission shall consist of four members: - the Supreme Judge (hereinafter: the Supreme Judge) of the Supreme Court of the Republic of Slovenia, who is the President of the Commission, - the Supreme State Prosecutor (of the Supreme State Prosecutor's Office of the Republic of Slovenia, - a representative of the ministry responsible for justice, - a representative of the ministry responsible for the interior.	
Which LEAs can use this tool?	primarily by the Police, but in case that the witness is imprisoned: the Administration for the Execution of Criminal Sanctions, the Administration of the Prison Enforcement Institution, the Penitentiary Institution juvenile imprisonment or an institution for the enforcement of educational measures	
What are the rules to be followed for the implementation of this tool?	Article 10 in ZZPrič: (1) For the protection of protected persons by law, the following conditions must be met: 1. that pre-trial or criminal proceedings are pending for a criminal offense in respect of which, in accordance with the provisions of the law governing criminal proceedings, covert investigative measures may be ordered by a court decision; 2. that the witness knows how to tell about the crime from the previous points, the perpetrator or other important environment; 3. that the offense cannot be investigated or proven or that the offenses cannot be further enforced, prevented without the participation of this story in pre-trial or criminal proceedings; 4. that the participation of the stories poses a serious danger to her life or the body or the lives of other physical persons; 5. not to take the risk of cooperating with agricultural groups without implementing emergency safeguards or protecting programs under the law in 6. that, on the basis of the assessment of the unit, the possibility of successful implementation of the protection program has been determined. (2) The condition referred to in point 2 of the preceding paragraph must be proved by the minutes of the statement given by the witness before the competent state prosecutors or the prosecutor (hereinafter: the prosecutor). The record shall state what testifies to the punishment of the act, the perpetrator, or other significant circumstances. (3) Before submitting the statement referred to in the preceding paragraph, the state prosecutor shall list the witness with the rights and duties they had during the hearing in the proceedings under the provisions of the law governing criminal proceedings. (4) The state prosecutor shall list the suspect or accused referred to in Article 4 of this Act before submitting the statement referred to in the second paragraph of this Article with his rights in the proceedings and with the possibility of mitigating the sentence due to the provision of the law governing criminal proceedings.	• ZZPrič (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4265
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	The Commission for the Protection of Endangered Persons	
What ongoing supervision is required for the use of this tool?	Types of supervision are defined in Article 28, 29, 30 of ZZPrič: Article 38 (1) Supervision over the substantive documentation regarding the use of financial resources may be exercised only by the commission. (2) The control of the use of financial or budgetary funds carried out by other authorised bodies may only include a review of the accounting documentation. Content and administrative control. Article 39 (1) Supervision over the work of the commission shall be exercised by the President of the Supreme Court of the Republic of Slovenia or by the Supreme Judge authorised by him in writing. (2) The substantive control over the work of the unit shall be performed by the commission. The Commission may inspect the unit's documentation in relation to the control referred to in the previous paragraph. (3) Administrative control over the work of the unit shall be performed by the competent authorities.	• ZZPrič (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4265

Relevant items	Provisions	Sources used
	(4) The minutes on the performed supervision shall be forwarded to the commission or unit, which is obliged to eliminate the established irregularities and deficiencies and to report thereon to the body that performed the supervision within a specified time limit. Manner of performing control. Article 40 Supervision under this chapter must be performed in a manner that does not allow the disclosure of endangered or protected persons.	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Surveillance		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Procedure Act (ZKP), Official Gazette no. 32/12 – consolidated version, no. 47/13, 87/14, 8/16 – Constitutional Court decision, 64/16 – Constitutional Court decision, 65/16 – Constitutional Court decision, 66/17 – ORZKP153,154, 22/19, 55/20 – Constitutional Court decision, 89/20 – Constitutional Court decision, 191/20 – Constitutional Court decision and no. 200/20) Cooperation in Criminal Matters with the Member States of the European Union Act (ZSKZDČEU-1), Official Gazette of Republic of Slovenia no. 48/13, 37/15 in 22/18 Agreement between the Republic of Slovenia and the Republic of Austria on Police Cooperation (BATPS) Agreement between the Republic of Slovenia and the Republic of Hungary on cross-border co-operation of law enforcement authorities (BHUCPS) Agreement between the Republic of Slovenia and the Republic of Italy on cross-border police cooperation (BITČPS) Agreement between the Republic of Slovenia and the Republic of Croatia on Cross-border police co-operation (BHRPS) Police Cooperation Convention for Southeast Europe (Official Gazette of Republic of Slovenia no. 18/12) (MKPS)	• ZKP (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362# • ZKP (English - not all changes and amendments are included) https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf • Cooperation Act (Slovenian): http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6513 • Cooperation Act (English): https://www.ejtn.eu/PageFiles/6533/2014%20seminars/Nicosia/SI_Legislation/Law_Cooperation_Criminal_Matters.pdf • BATPS (Slovenian & German): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2004-02-0052/#I.%C2%A0poglavjeSplo%C5%A1ne%C2%A0dolo%C4%8Dbe • BHUCPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0029?sop=2007-02-0029 • BITČPS (Slovenian & Italian): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0134?sop=2007-02-0134 • BHRPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2003-02-0014?sop=2003-02-0014 • MKPS (English) https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2012-02-0103/zakon-o-ratifikaciji-konvencije-o-policijskem-sodelovanju-v-jugovzhodni-evropi-mkps
Specific range of application of the tool	Article 149a: - continual or repeat sessions of surveillance or pursuit using technical devices for establishing position or movement and technical devices for transmitting and recording sound, photography and video recording, and shall focus on monitoring the position, movement and activities of a person from the preceding paragraphs.	• ZKP (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362# • ZKP (English - not all changes and amendments are included) https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf
How is the tool defined?	Article 149a in ZKP (1) If there are reasonable grounds for suspecting that a certain person has committed, is committing, is preparing to commit or is organising the commission of any of the criminal offences specified in the fourth paragraph of this article and if it is reasonable to conclude that police officers would be unable to uncover, prevent or prove this offence using other measures, or if these other measures would give rise to disproportionate difficulties, secret surveillance of this person may be ordered. (2) Secret surveillance may also exceptionally be ordered against a person who is not a suspect if it is reasonable to conclude that surveillance of this person will lead to the identification of a suspect from the preceding paragraph whose personal data is unknown, to the residence or whereabouts of a suspect from the preceding paragraph, or to the residence or whereabouts of a person who was ordered into custody, ordered to undergo house arrest or had an arrest warrant or an order to appear issued against him but who escaped or is in hiding and police officers are unable to obtain this information by other measures, or if these other measures would give rise to disproportionate difficulties. (3) Secret surveillance shall be carried out as continual or repeat sessions of surveillance or pursuit using technical devices for establishing position or movement and technical devices for transmitting and recording sound, photography and video recording, and shall focus on monitoring the position, movement and activities of a person from the preceding paragraphs. Secret surveillance may be carried out in public and publicly accessible open and closed premises, as well places and premises that are visible from publicly accessible places or premises. Under	• ZKP (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362# • ZKP (English - not all changes and amendments are included) https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf • Cooperation Act (Slovenian): http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6513 • Cooperation Act (English): https://www.ejtn.eu/PageFiles/6533/2014%20seminars/Nicosia/SI_Legislation/Law_Cooperation_Criminal_Matters.pdf • BATPS (Slovenian & German): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2004-02-0052/#I.%C2%A0poglavjeSplo%C5%A1ne%C2%A0dolo%C4%8Dbe • BHUCPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0029?sop=2007-02-0029 • BITČPS (Slovenian & Italian): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0134?sop=2007-02-0134 • BHRPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2003-02-0014?sop=2003-02-0014 • MKPS (English) https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2012-02-0103/zakon-o-ratifikaciji-konvencije-o-policijskem-sodelovanju-v-jugovzhodni-evropi-mkps

Relevant items	Provisions	Sources used
	conditions from this article, secret surveillance may also be carried out in private premises if the owner of these premises so allows. (4) The criminal offences for which secret surveillance may be ordered are as follows: 1) criminal offences for which the law prescribes a prison sentence of five or more years; 2) criminal offences from point 2 of the second paragraph of Article 150 of this Act and the criminal offences of false imprisonment (Article 143 of the Penal Code), threatening the safety of another person (Article 145), fraud (Article 217), concealment (Article 221), disclosure of and unauthorised access to trade secrets (Article 241), abuse of inside information (Article 243), fabrication and use of counterfeit stamps of value or securities (Article 250), forgery (Article 256), special cases of forgery (Article 257), abuse of office or official rights (Article 261), disclosure of an official secret (Article 266), being an accessory after the fact (Article 287), endangering the public (Article 317), pollution and destruction of the environment (Article 333), bringing of hazardous substances into the country (Article 335), pollution of drinking water (Article 337), and tainting of foodstuffs or fodder (Article 338). (5) Secret surveillance shall be permitted by the state prosecutor on the basis of a written order and at the written request of the police, except in cases from the sixth paragraph of this article, when an order must be obtained from the investigating judge. (6) Secret surveillance shall be ordered in writing by the investigating judge, at the written request of the state prosecutor, in the following cases: 1) if he envisages the use of technical devices for the transmission and recording of sound in the application of the measure, where this measure may be ordered only for criminal offences from the second paragraph of Article 150 of this Act; 2) if application of the measure requires the installation of technical devices in a vehicle or in other protected or closed premises or objects in order to establish the position and movements of a suspect; 3) for application of a measure in private premises, if the owner of these premises so allows; 4) for the application of a measure against a person who is not a suspect (second paragraph of this article). (7) Proposals and orders shall be constituent parts of criminal files and must contain: 1) information that allows the person against whom the measure is being requested or ordered to be identified accurately; 2) reasonable grounds or the adducement of reasonable grounds for suspicion; 3) in the case from the second paragraph of this article, information that allows a suspect from the first paragraph of this article to be identified accurately, and the establishment of probability that application of the measure will lead to the identification of the suspect, his whereabouts or his place of residence; 4) the written consent of the owner of the private premises in which the measure will be applied; 5) the method of application, the scope and the duration of the measure, and other important circumstances that dictate use of the measure; 6) the grounds for or establishment of need to use the measure in question as opposed to another method of gathering information. (8) In exceptional cases, if written orders cannot be obtained in time and if a delay would present a risk, the state prosecutor may, in the case from the fifth paragraph of this article and at the verbal request of the police, allow the measure to commence on the basis of a verbal order; in the case from the sixth paragraph of this article, the investigating judge may, at the verbal request of the state prosecutor, allow the measure to commence on the basis of a verbal order. The body that issued the verbal order shall make an official note of the verbal request. A written order, which must contain the reason why the measure has been commenced before time, must be issued within 12 hours of the issuing of the verbal order at the latest. Reasonable grounds must exist for application of the measure before time; if this is not the case, the court shall always act in accordance with the fourth paragraph of Article 154 of this Act regardless of whether the use of measures is otherwise justified. (9) If a person against whom a measure is being applied comes into contact with an unidentified person in relation to whom there are reasonable grounds for suspecting that he is involved in criminal activity connected with the criminal offences for which the measure is being applied, the police may also place this person under secret surveillance without the need to obtain the order from the fifth or sixth paragraphs of this article if this is urgently required in order to establish the identity of this person or obtain other information important for criminal proceedings. The police must obtain prior verbal permission from the state prosecutor for such surveillance, unless it is impossible to obtain permission on time and any delay would present a risk. In this case the police shall, as soon as possible and within six hours of commencement of application of the measure at the latest, inform the state prosecutor, who may prohibit further application of the measure if he believes that there are no reasonable grounds for it. This measure may last for a maximum of 12 hours from contact with the person against whom the measure is being applied. When applying the measure from this paragraph, the police may not use technical equipment	

Relevant items	Provisions	Sources used
	and devices from points 1 and 2 of the sixth paragraph of this article, nor may they apply the measure in private premises. The police shall make an official note immediately after the cessation of such surveillance and send it without delay to the state prosecutor that granted the permission from this paragraph and to the body that issued the original secret surveillance order. The official note shall become part of the criminal file. (10) Application of a measure may last a maximum of two months. If due cause is adduced, it may be extended every two months by means of a written order. The measure may last a total of: 1) six months in the case from the sixth paragraph of this article; 2) 24 months in cases from the fifth paragraph of this article if they relate to criminal offences from the fourth paragraph of this article, and 36 months if they relate to criminal offences from the second paragraph of Article 151 of this Act. (11) The police shall cease application of the measure as soon as the reasons for which the measure was ordered are no longer in place. The police shall notify the body that ordered the measure of the cessation without delay and in writing. The police shall send the body that ordered the measure a monthly report on the progress of the measure and the information obtained. The body that ordered the measure may, at any time and on the basis of this report or ex officio, order in writing that application of the measure be halted if it assesses that the reasons for the measure are no longer in place or if the measure is being applied in contravention of its order. (12) If a measure is applied against the same person for more than six months, the panel (sixth paragraph of Article 25) shall review the legality of and grounds for application of the measure upon the first extension over six months and every further six months thereafter. The body that issued the extension order shall send the panel all the relevant material; the panel shall decide within three days. If the panel assesses that there are no grounds for application of the measure or that all the legal conditions have not been fulfilled, it shall issue a decision ordering that the measure come to an end. There shall be no appeal against this decision. (13) The police must carry out secret surveillance in a way that encroaches on the rights of persons that are not suspects to the smallest possible extent Bilateral agreements are listed below: Article 7 in BATPS (1) The security authorities of a Contracting Party which, as part of an investigation into a criminal offense in their country, secretly observes and tracks a person suspected of a criminal offense for which extradition may be requested may continue covert surveillance and tracing in the territory of the other Contracting Party on the basis of a prior request. Approval may be subject to additional conditions. At the request of the competent authorities of the Contracting Party in whose territory the covert surveillance is being carried out, this shall be left to the officials of that Contracting Party. (2) A request in accordance with the first paragraph of this Article must be forwarded to: - in the Republic of Slovenia, the Ministry of the Interior, the General Police Administration, the Criminal Police Administration, and - in the Republic of Austria, the Federal Ministry of the Interior, the Directorate-General for Public Security, the Federal Criminal Bureau. (3) If, due to the special urgency of the case of the other Contracting Party, it is not possible to apply for approval in advance, cross-border covert surveillance and tracking may continue across the state border, provided that the border crossing is immediately communicated to the competent authority of that Contracting Party, in whose territory it will continue. The following must be notified of the crossing of the border: - in the Republic of Slovenia, the Kranj Police Administration or the Slovenj Gradec Police Administration or the Celje Police Administration or the Maribor Police Administration or the Murska Sobota Police Administration, if it falls within their local jurisdiction, - in the Republic of Austria, the Security Directorate for the Land of Burgenland or the Security Directorate for the Land of Carinthia or the Security Directorate for the Land of Styria, if it falls within their territorial jurisdiction. A request pursuant to the first paragraph of this Article, which must state the reasons for crossing the state border without prior approval, must be forwarded immediately. Covert surveillance and tracking shall be terminated as soon as the Contracting Party in whose territory this is carried out so requests upon notification or request, or if approval has not been obtained within twelve hours after crossing the national border. (4) For the purpose of conducting covert surveillance and tracking, a Contracting Party may, with the approval of the other Contracting Party, also use aircraft or watercraft. (5) Secret observation and tracking in accordance with the first and third paragraphs of this Article is permitted only under the following conditions: a) officials conducting secret surveillance and surveillance shall be bound by the provisions of this Article and by the national law of the Contracting Party in whose territory they operate. They must comply with the orders of the local competent authorities;	

Relevant items	Provisions	Sources used
	b) except in the case referred to in paragraph 3 of this Article, during secret surveillance and surveillance, officials must carry a document showing that the permit has been obtained; c) officials carrying out covert surveillance must always be able to prove their official function; d) officials carrying out covert surveillance and surveillance may carry their service weapons during such surveillance, unless the requested Party expressly objects. The use of weapons is only allowed in the silobran; e) entry into dwellings and publicly inaccessible land is not allowed. Entry into publicly accessible working, operating and business premises is possible during their working, operating and business hours; f) officials conducting secret surveillance and tracking are not authorised to detain, apprehend or apprehend a person under secret surveillance and tracking; g) a report shall be submitted to the Party in whose territory this was carried out for any covert surveillance and tracking. The personal presence of the officials who carried out the secret surveillance and tracking may also be required; h) upon request, the authorities of the Party from which the officials conducting the secret surveillance and tracing come shall provide support for the subsequent investigation, including the legal proceedings of the Party in whose territory the secret surveillance and tracking took place; i) the technical means necessary to carry out covert surveillance may be used to the extent necessary in accordance with the national law of the Contracting Party in whose territory it is carried out. The technical means used for covert surveillance and tracking must be specified in the request referred to in the first paragraph of this Article; j) the vehicles used are, in terms of exemption from traffic bans and traffic restrictions, equivalent to those of the security authorities of the Contracting Party in whose territory they are used. Signalling may be used if necessary for the purpose of conducting covert surveillance and tracking. (6) Cross-border covert surveillance and tracking shall be carried out without spatial restrictions. Article 11 in BHUČPS 1. In the course of investigation in their national territory, the authorised co-operating authorities of the Contracting Parties shall be authorised to continue surveillance in the territory of the other Contracting Party if its central contact point has authorised this in response to a prior request and if this concerns a person who has been suspected of engagement in an organised criminal group or suspected of intentionally committing a criminal act sanctioned with imprisonment of at least five years or a person who has been associated with them or is about to establish contact with them. Conditions may be attached to the authorisation. 2. In case of suspicion of criminal acts specified in Paragraph (1), the authorised co-operating authorities of the Contracting Parties may pursue the surveillance of the person in contact with the perpetrator when there is reason to believe that this person may assist in the identification or finding of the perpetrator or may lead to the perpetrator. 3. Upon request of the authorised co-operating authorities of the requested Contracting Party, the continuation of surveillance shall be transferred immediately to the authorised co-operating authority of the requested Contracting Party. Upon request, the Contracting Parties may mutually assist one another in conducting surveillance. 4. The authorisation for surveillance shall be valid to the entire territory of the states of the Contracting Parties. In the course of surveillance the common state border of the Contracting Parties may also be crossed outside border crossing points and business hours. 5. In the event that a delay would give rise to danger or jeopardise the interests of criminal investigation, surveillance may be continued even without the advance authorisation stipulated in Paragraph (1). In this case the competent authorised co-operating authorities of the requested Contracting Party shall be notified immediately upon crossing the state border. The request shall be sent subsequently but without delay to the central contact point of the requested Contracting Party. The request shall indicate the reasons for crossing the border without prior authorisation. 6. The competent authorised co-operating authorities referred to in Paragraph (5) shall be: a) for the Slovenian Contracting Party: – Ministry of the Interior, Police, General Police Directorate; b) for the Hungarian Contracting Party: – National Police Headquarters. 7. Surveillance according to Paragraph (5) shall cease immediately if so requested by the authorised co-operating authority of the requested Contracting Party, or where the authorisation, necessary for the execution of the request, has not been obtained within five hours from crossing the border. 8. Surveillance may be carried out only under the following conditions: a) the officers conducting surveillance shall comply with the provisions of this Article and with the internal laws and regulations of the Contracting Party on whose territory they are operating;	

Relevant items	Provisions	Sources used
	they shall act in accordance with the instructions of the authorised co-operating authority with territorial competence; b) except in situations provided for in Paragraph (5), the officer conducting surveillance shall carry a document verifying that the surveillance has been authorised; c) the officer conducting surveillance must be able at all times to prove that he is acting in an official capacity; d) the officer conducting surveillance may not enter a private home or places not accessible to the public, but may enter work premises, service and business premises and areas which are accessible to the public during working hours; e) the officer conducting surveillance shall submit a report to the central contact point of the requested Contracting Party; f) when technical instruments are also needed for conducting surveillance, they may be used when that is permitted under the laws and regulations of the requested Contracting Party. The request according to Paragraph (1) shall specify the technical instruments of surveillance to be applied; g) the use of vehicles for surveillance shall be subject to the traffic regulations of the requested Contracting Party. Article 6 in BITCPS 1. The security authorities of a Contracting Party which, in the course of an investigation into a criminal offense in their country, secretly observe and track a person suspected of a criminal offense for which extradition may be requested may continue covert surveillance and tracing in the territory of the other Contracting Party if asked for approval. Approval may be subject to additional conditions. At the request of the competent authorities of the Contracting Party in whose territory the covert surveillance and tracing is being carried out, this shall be left to the latter or shall be terminated immediately. 2. The request referred to in the previous paragraph must be sent: - in the Republic of Slovenia: the Ministry of the Interior, the Police, the General Police Administration, the Criminal Police Administration; - in the Italian Republic: the Ministry of the Interior, the Public Security Administration, the Central Directorate of Criminal Police - the International Police Cooperation Service. 3. If, due to the special urgency of the case of the other Contracting Party, it is not possible to apply for authorisation in advance, cross-border covert surveillance and surveillance may continue across the border, under condition that the competent authority of the Contracting Party in whose territory they continue shall be notified without delay of the crossing of the State border during covert surveillance and tracing. The following must be notified of the crossing of the border: - in the Republic of Slovenia: the Ministry of the Interior, the Police, the General Police Administration, the Criminal Police Administration, the Sector for International Police Cooperation; - in the Italian Republic: the Ministry of the Interior, the Public Security Administration, the Central Directorate of Criminal Police - Service for International Police Cooperation, and the Center for Police Cooperation Vrata - Megvarje. The request referred to in the first paragraph, stating the reasons that led to the crossing of the state border without prior approval, must be sent immediately. Covert surveillance and tracking shall be discontinued as soon as the Contracting Party in whose territory they are conducting so requests upon notification or request, or if approval has not been obtained within twelve hours after crossing the national border. 4. For the purpose of conducting covert surveillance and tracking, a Party may, with the approval of the other Party, also use aircraft or watercraft. 5. Covert surveillance and surveillance shall be permitted in accordance with paragraphs 1 and 3 of this Article only under the following conditions: a) Officials shall comply with the provisions of this Article and the domestic law of the Contracting Party in whose territory they operate. They must comply with the orders of the local competent authorities; b) except in the case referred to in paragraph 3, officials must carry a document showing that the permit has been obtained; c) officials must always be able to prove their official position; d) officials carrying out covert surveillance and tracking may carry their service weapons, unless the requested Party expressly objects. The use of weapons is only allowed in the silobran; e) entry into dwellings and places not accessible to the public is not permitted. Entry into publicly accessible working, operating and business premises is possible during their working, operating or business hours; f) officials are not authorised to stop, apprehend or apprehend a person who is secretly observed and followed;	

Relevant items	Provisions	Sources used
	g) officials of the Contracting Parties shall report any covert surveillance and tracing in the territory of the other Contracting Party to the authorities of the other Contracting Party referred to in paragraph 2. If the circumstances of the case so require, the personal presence of the officials who carried out the secret surveillance and tracking may also be requested; h) the authorities of the Contracting Party from which the officials conducting the covert surveillance and tracking come on request shall provide assistance in continuing the investigation; i) the technical means necessary to carry out covert surveillance and tracking may be used to the extent necessary in accordance with the domestic law of the Contracting Party in whose territory it is carried out. The technical means used for covert surveillance and tracking must be specified in the request referred to in the first paragraph; j) the vehicles used are equated with the vehicles of the security authorities of the Contracting Party in whose territory they are used in terms of exemption from traffic bans and traffic restrictions. Signalling may be used if required for covert surveillance and tracking. 6. Cross-border covert surveillance and tracking shall be carried out without spatial restriction. Article 14 of MKPS (1) Officers of one of the Contracting Parties who, as part of a criminal investigation, are keeping under surveillance in their country a person who is presumed to have participated in an extraditable criminal offence shall subject to bilateral Implementation Agreements concluded in accordance with Article 34 paragraph 1 of this Convention be authorised to continue their surveillance in the territory of another Contracting Party where the latter has authorised cross-border surveillance in response to a request for assistance made in advance. Conditions may be attached to the authorisation. On request, the surveillance will be entrusted to officers of the Contracting Party in whose territory this is carried out. The request for assistance referred to in the first subparagraph must be sent to an authority designated by each of the Contracting Parties and empowered to grant or to pass on the requested authorisation. (2) Where, for particularly urgent reasons, prior request for authorisation cannot be submitted from the requesting Contracting Party, the Officers carrying out the surveillance shall subject to bilateral Implementation Agreements mentioned in paragraph 1 of this Article be allowed to continue beyond the border the surveillance of a person presumed to have committed a criminal offence as mentioned in paragraph 3. In these cases, the authority of the Contracting Party in whose territory the surveillance is to be continued, must be notified immediately that the border has been crossed, and a request for assistance outlining the grounds for crossing the border without prior authorisation shall be submitted with no delay. (3) The bilateral Implementation agreements as referred to in paragraphs 1 and 2 of this Article shall define the criminal offences mentioned in paragraph 2 either by way of an exhaustive list or by extending it to all extraditable criminal offences. (4) Surveillance shall cease as soon as the Contracting Party in whose territory it is taking place so requests, following the notification or the request referred to in the previous paragraphs, where authorisation has not been obtained, five hours after the border was crossed. (5) The surveillance referred to in paragraphs 1 and 2 shall be carried out only under the following general conditions: a) The officers carrying out the surveillance must comply with the provisions of this Article and with the law of the Contracting Party in whose territory they are operating; they must obey the instructions of the competent local authorities. b) Except in the situations outlined in paragraph 2, the officers shall, during the surveillance, carry a document certifying that authorisation has been granted. c) The officers carrying out the surveillance must at all times be able to prove that they are acting in an official capacity. d) The officers carrying out the surveillance may carry their service weapons during the surveillance unless specifically otherwise decided by the requested Party; their use shall be prohibited except in cases of legitimate self-defence. e) Entry into private homes and places not accessible to the public is prohibited. f) The officers carrying out the surveillance may neither challenge nor arrest the person under surveillance. g) All operations shall be the subject of a report to the authorities of the Contracting Party in whose territory they took place; the officers carrying out the surveillance may be required to appear in person. h) The authorities of the Contracting Party from which the surveillance officers have come shall, when requested by the authorities of the Contracting Party in whose territory the surveillance took place, assist the enquiry subsequent to the operation in which they took part, including judicial proceedings, provided that the identity of the involved officer is protected. (6) The officers referred to in the previous paragraphs shall be specified in the bilateral Implementation Agreements.	

Relevant items	Provisions	Sources used
	(7) The Contracting Parties may, by way of bilateral Implementation Agreement, extend the scope of this Article and adopt additional measures in application thereof.	
For what types of crime can the tool be used?	Article 149.an in ZKP (4) The criminal offences for which secret surveillance may be ordered are as follows: 1) criminal offences for which the law prescribes a prison sentence of five or more years; 2) criminal offences from point 2 of the second paragraph of Article 150 of this Act (and the criminal offences of false imprisonment (Article 143 of the Penal Code), threatening the safety of another person (Article 145), fraud (Article 217), concealment (Article 221), disclosure of and unauthorised access to trade secrets (Article 241), abuse of inside information (Article 243), fabrication and use of counterfeit stamps of value or securities (Article 250), forgery (Article 256), special cases of forgery (Article 257), abuse of office or official rights (Article 261), disclosure of an official secret (Article 266), being an accessory after the fact (Article 287), endangering the public (Article 317), pollution and destruction of the environment (Article 333), bringing of hazardous substances into the country (Article 335), pollution of drinking water (Article 337), and tainting of foodstuffs or fodder (Article 338). Point 2, second paragraph of Article 150 2) the criminal offence of kidnapping under Article 144, the showing, possession, manufacture and distribution of pornographic material under Article 187,illegal production of and trade in drugs under Article 196, enabling the taking of drugs under Article 197, blackmail under Article 218, abuse of inside information under Article 243, unlawful acceptance of gifts under Article 247, unauthorised giving of gifts under Article 248, money laundering under Article 252, smuggling under Article 255, accepting of a bribe under Article 267, giving of a bribe under Article 268, acceptance of gifts to secure unlawful intervention under Article 269, giving of gifts to secure unlawful intervention under Article 269a, criminal association under Article 297, illegal manufacture of and trade in arms or explosives under Article 310, and causing danger with nuclear substances under Article 319 of the Penal Code of the Republic of Slovenia;	• ZKP (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362# • ZKP (English - not all changes and amendments are included) https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf
Does national law allow this tool to be used in cross border cases?	Yes, Criminal procedure act is not specific about it, but the tool is part of bilateral agreements.	
What thresholds must be passed for the use of this tool?	In principle a prison sentence of five or more years, other criminal offences are listed specifically: Article 149.a in ZKP (4) The criminal offences for which secret surveillance may be ordered are as follows: 1) criminal offences for which the law prescribes a prison sentence of five or more years; 2) criminal offences from point 2 of the second paragraph of Article 150 of this Act and the criminal offences of false imprisonment (Article 143 of the Penal Code), threatening the safety of another person (Article 145), fraud (Article 217), concealment (Article 221), disclosure of and unauthorised access to trade secrets (Article 241), abuse of inside information (Article 243), fabrication and use of counterfeit stamps of value or securities (Article 250), forgery (Article 256), special cases of forgery (Article 257), abuse of office or official rights (Article 261), disclosure of an official secret (Article 266), being an accessory after the fact (Article 287), endangering the public (Article 317), pollution and destruction of the environment (Article 333), bringing of hazardous substances into the country (Article 335), pollution of drinking water (Article 337), and tainting of foodstuffs or fodder (Article 338). Point 2, second paragraph of Article 150 2) the criminal offence of kidnapping under Article 144, the showing, possession, manufacture and distribution of pornographic material under Article 187,illegal production of and trade in drugs under Article 196, enabling the taking of drugs under Article 197, blackmail under Article 218, abuse of inside information under Article 243, unlawful acceptance of gifts under Article 247, unauthorised giving of gifts under Article 248, money laundering under Article 252, smuggling under Article 255, accepting of a bribe under Article 267, giving of a bribe under Article 268, acceptance of gifts to secure unlawful intervention under Article 269, giving of gifts to secure unlawful intervention under Article 269a, criminal association under Article 297, illegal manufacture of and trade in arms or explosives under Article 310, and causing danger with nuclear substances under Article 319 of the Penal Code of the Republic of Slovenia;	• ZKP (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362# • ZKP (English - not all changes and amendments are included) https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf
What types of stakeholder are involved in the implementation of this tool?	In all cases surveillance is performed by the police. Bilateral agreements define point of contact for each agreement. (See below) Article 7 in BATPS - The security authorities conducting the surveillance; -A request must be submitted to: - in the Republic of Slovenia, the Ministry of the Interior, the General Police Administration, the Criminal Police Administration, and in the Republic of Austria, the Federal Ministry of the Interior, the Directorate-General for Public Safety, the Federal Criminal Bureau. Article 1 in BATPS in connection to Article 9 in BATPS	• BATPS (Slovenian & German): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2004-02-0052/#I.%C2%A0poglavjeSplo%C5%A1ne%C2%A0dolo%C4%8Dbe • BHUCPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0029?sop=2007-02-0029 • BITCPS (Slovenian & Italian): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0134?sop=2007-02-0134 • BHRPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2003-02-0014?sop=2003-02-0014

Relevant items	Provisions	Sources used
	(3) The security authorities under this Treaty are: in the Republic of Slovenia, the Ministry of the Interior, the General Police Administration, as the national central service with its internal organisational units and regional organisational units of the police (hereinafter: police administrations) within its competences, in the Republic of Austria, the Federal Minister of the Interior as the national central service, the security directorates, the federal police directorates and, outside the area of territorial competence of the federal police directorates, the district administrative bodies. Article 12 in BHUCPS 6. The competent authorised bodies for cooperation conducting the surveillance are: - for the Slovenian Contracting Party: - Ministry of the Interior, Police, General Police Administration; - for the Hungarian Contracting Party: - Chief State Police Captainty. Article 8 in BITCPS - The security authorities conducting the surveillance; - (2) In the case of the surveillance, the following shall be informed: - in the Republic of Slovenia: the Ministry of the Interior, the Police, the General Police Administration, the Criminal Police Administration; - in the Italian Republic: the Ministry of the Interior, the Public Security Administration, the Central Directorate of Criminal Police - the International Police Cooperation Service. - (3). If, due to the special urgency of the case of the other Contracting Party, it is not possible to apply for authorisation in advance, cross-border clandestine surveillance and tracing may continue beyond the state border, provided that the competent authority is immediately informed Contracting Parties in whose territory they will continue. The following must be notified of the crossing of the border: - in the Republic of Slovenia: Ministry of the Interior, Police, General Police Administration, Criminal Police Administration, Sector for International Police Cooperation; - in the Italian Republic: the Ministry of the Interior, the Public Security Administration, the Central Directorate of Criminal Police - Service for International Police Cooperation, and the Center for Police Cooperation Vrata - Megvarje. Article 1 in BITCPS in connection to Article 8 3. The security authorities under this Agreement are: in the Republic of Slovenia: the Ministry of the Interior, the Police, the General Police Administration as a national central body with its internal organisational units and regional police organisational units (hereinafter referred to as the Police Administration) within their competences; in the Italian Republic: the Ministry of the Interior, the Public Security Administration as the national central authority and the regional offices within their competences. Article 13 in MKPS - Officers of one of the Contracting Parties who are conducting the surveillance; - The authority of the Contracting Party in whose territory the surveillance is to be continued, must be notified	• MKPS (English) https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2012-02-0103/zakon-o-ratifikaciji-konvencije-o-policijskem-sodelovanju-v-jugovzhodni-evropi-mkps
Which LEAs can use this tool?	Police	
What are the rules to be followed for the implementation of this tool?	Rules listed in Slovenian legislation: Article 149a in ZKP (13) The police must carry out secret surveillance in a way that encroaches on the rights of persons that are not suspects to the smallest possible extent. Article 7 in BATPS 5) Covert surveillance and tracking in accordance with the first and third paragraphs of this Article is permitted only under the following conditions: a) officials conducting secret surveillance and surveillance shall be bound by the provisions of this Article and by the national law of the Contracting Party in whose territory they operate. They must comply with the orders of the local competent authorities; b) except in the case referred to in paragraph 3 of this Article, during secret surveillance and surveillance, officials must carry a document showing that the permit has been obtained; c) officials carrying out covert surveillance must always be able to prove their official function; d) officials carrying out covert surveillance and surveillance may carry their service weapons during such surveillance, unless the requested Party expressly objects. The use of weapons is only allowed in the silobran; e) entry into dwellings and publicly inaccessible land is not allowed. Entry into publicly accessible working, operating and business premises is possible during their working, operating and business hours; f) officials conducting secret surveillance and tracking are not authorised to detain, apprehend or apprehend a person under secret surveillance and tracking;	• BATPS (Slovenian & German): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2004-02-0052/#I.%C2%A0poglavjeSplo%C5%A1ne%C2%A0dolo%C4%8Dbe • BHUCPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0029?sop=2007-02-0029 • BITCPS (Slovenian & Italian): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0134?sop=2007-02-0134 • BHRPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2003-02-0014?sop=2003-02-0014 • MKPS (English) https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2012-02-0103/zakon-o-ratifikaciji-konvencije-o-policijskem-sodelovanju-v-jugovzhodni-evropi-mkps

Relevant items	Provisions	Sources used
	g) a report shall be submitted to the Party in whose territory this was carried out for any clandestine surveillance and tracking. The personal presence of the officials who carried out the secret surveillance and tracking may also be required; h) the authorities of the Contracting Party from which the secret surveillance and tracking officials come shall, upon request, provide support for the subsequent investigation, including the legal proceedings of the Contracting Party in whose territory the covert surveillance and tracking took place; i) the technical means necessary to carry out covert surveillance and surveillance may be used to the extent necessary in accordance with the national law of the Contracting Party in whose territory it is carried out. The technical means used for covert surveillance and tracking must be specified in the request referred to in the first paragraph of this Article; j) the vehicles used are, in terms of exemption from traffic bans and traffic restrictions, equivalent to those of the security authorities of the Contracting Party in whose territory they are used. Signalling may be used if necessary for the purpose of conducting covert surveillance and tracking. Article 6 in BITČPS 5. Covert surveillance and surveillance shall be permitted in accordance with paragraphs 1 and 3 of this Article only under the following conditions: a) Officials shall comply with the provisions of this Article and the domestic law of the Contracting Party in whose territory they operate. They must comply with the orders of the local competent authorities; b) except in the case referred to in paragraph 3, officials must carry a document showing that the permit has been obtained; c) officials must always be able to prove their official position; d) officials carrying out covert surveillance and tracking may carry their service weapons, unless the requested Party expressly objects. The use of weapons is only allowed in the silobran; e) entry into dwellings and places not accessible to the public is not permitted. Entry into publicly accessible working, operating and business premises is possible during their working, operating or business hours; f) officials are not authorised to stop, apprehend or apprehend a person who is secretly observed and followed; g) officials of the Contracting Parties shall report on any covert surveillance and tracing in the territory of the other Contracting Party to the authorities of the other Contracting Party referred to in paragraph 2. If the circumstances of the case so require, the personal presence of the officials who carried out the secret surveillance and tracking may also be requested; h) the authorities of the Contracting Party from which the officials conducting the covert surveillance and tracking come on request shall provide assistance in continuing the investigation; i) the technical means necessary to carry out covert surveillance and tracking may be used to the extent necessary in accordance with the domestic law of the Contracting Party in whose territory it is carried out. The technical means used for covert surveillance and tracking must be specified in the request referred to in the first paragraph; j) the vehicles used are equated with the vehicles of the security authorities of the Contracting Party in whose territory they are used in terms of exemption from traffic bans and traffic restrictions. Signalling may be used if required for covert surveillance and tracking. Article 14 in MKPS (5) The surveillance referred to in paragraphs 1 and 2 shall be carried out only under the following general conditions: a) The officers carrying out the surveillance must comply with the provisions of this Article and with the law of the Contracting Party in whose territory they are operating; they must obey the instructions of the competent local authorities. b) Except in the situations outlined in paragraph 2, the officers shall, during the surveillance, carry a document certifying that authorisation has been granted. c) The officers carrying out the surveillance must at all times be able to prove that they are acting in an official capacity. d) The officers carrying out the surveillance may carry their service weapons during the surveillance unless specifically otherwise decided by the requested Party; their use shall be prohibited except in cases of legitimate self-defence. e) Entry into private homes and places not accessible to the public is prohibited. f) The officers carrying out the surveillance may neither challenge nor arrest the person under surveillance. g) All operations shall be the subject of a report to the authorities of the Contracting Party in whose territory they took place; the officers carrying out the surveillance may be required to appear in person.	

Relevant items	Provisions	Sources used
	h) The authorities of the Contracting Party from which the surveillance officers have come shall, when requested by the authorities of the Contracting Party in whose territory the surveillance took place, assist the enquiry subsequent to the operation in which they took part, including judicial proceedings, provided that the identity of the involved officer is protected. Secretariat for MKPS prepared a manual for execution of the convention: 4.6. Practical regulations to carry out the surveillance 4.6.1. Before crossing the border - Even in urgent cases, a request for assistance shall be sent through the National Central Unit in each State. - In urgent cases a request shall be sent as soon as possible. - The submission of a request to cross the border shall be handled by the competent authorities in the requested State as a request for assistance according to Article 14 of the Convention. This request for assistance shall contain all the information as required by the bilateral agreement and shall be available at the time of the request. - An approval of the request must be given by the requested State. Certain conditions can be linked to the approval. 4.6.2. After crossing the border - The officer shall be subject to the laws and regulations in the State where he/she operates and follow the instructions from the competent authorities. - The officers carrying out the surveillance must at all times be able to give proof of their acting in an official capacity by using the attached form. - If the requested State does not oppose this explicitly, the officer is allowed to carry a service weapon, which can only be used in legitimate self-defence. - It is forbidden to enter domestic homes and places which are not open to the public. - The individual who is subject to surveillance should neither be arrested nor challenged by the foreign officers carrying out the surveillance. - In the event of a controlled delivery and if the competent law enforcement authorities of the requested Contracting Party cannot intervene in due time, and if continuation of the controlled delivery would present a serious risk for life or health of persons, or cause serious damage to property, or if the delivery could no longer be kept under control, the officer of the requesting Contracting Party can seize the controlled delivery. If necessary, the officers of the requesting Contracting Party can stop and apprehend persons who escort the shipment until intervention by law enforcement authorities of the requested Contracting Party. In any case the requesting Contracting Party shall inform the law enforcement authorities of the requested Contracting Party without delay. - The application shall be submitted to the National Central Unit before the surveillance starts. In urgent cases when the surveillance team crosses the border, the National Central Unit shall contact its counterpart. - The subject can however be retained and be submitted to a security search - which is not equivalent to an arrest - on condition that the subject has committed or taken part in the commission of an extraditable offence.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Time limitation of the measure. Paragraph 10 of Article 149.a (10) Application of a measure may last a maximum of two months. If due cause is adduced, it may be extended every two months by means of a written order. The measure may last a total of: 1) six months in the case from the sixth paragraph of this article; 2) 24 months in cases from the fifth paragraph of this article if they relate to criminal offences from the fourth paragraph of this article, and 36 months if they relate to criminal offences from the second paragraph of Article 151 of this Act.	• ZKP (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362# • ZKP (English - not all changes and amendments are included) https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Article 149a in ZKP (5) Secret surveillance shall be permitted by the state prosecutor on the basis of a written order and at the written request of the police, except in cases from the sixth paragraph of this article, when an order must be obtained from the investigating judge. (6) Secret surveillance shall be ordered in writing by the investigating judge, at the written request of the state prosecutor, in the following cases: 1) if he envisages the use of technical devices for the transmission and recording of sound in the application of the measure, where this measure may be ordered only for criminal offences from the second paragraph of Article 150 of this Act; 2) if application of the measure requires the installation of technical devices in a vehicle or in other protected or closed premises or objects in order to establish the position and movements of a suspect; 3) for application of a measure in private premises, if the owner of these premises so allows; 4) for the application of a measure against a person who is not a suspect (second paragraph of this article).	• ZKP (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362# • ZKP (English - not all changes and amendments are included) https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf

Relevant items	Provisions	Sources used
	(8) In exceptional cases, if written orders cannot be obtained in time and if a delay would present a risk, the state prosecutor may, in the case from the fifth paragraph of this article and at the verbal request of the police, allow the measure to commence on the basis of a verbal order; in the case from the sixth paragraph of this article, the investigating judge may, at the verbal request of the state prosecutor, allow the measure to commence on the basis of a verbal order. The body that issued the verbal order shall make an official note of the verbal request. A written order, which must contain the reason why the measure has been commenced before time, must be issued within 12 hours of the issuing of the verbal order at the latest. Reasonable grounds must exist for application of the measure before time; if this is not the case, the court shall always act in accordance with the fourth paragraph of Article 154 of this Act regardless of whether the use of measures is otherwise justified. (9) If a person against whom a measure is being applied comes into contact with an unidentified person in relation to whom there are reasonable grounds for suspecting that he is involved in criminal activity connected with the criminal offences for which the measure is being applied, the police may also place this person under secret surveillance without the need to obtain the order from the fifth or sixth paragraphs of this article if this is urgently required in order to establish the identity of this person or obtain other information important for criminal proceedings. The police must obtain prior verbal permission from the state prosecutor for such surveillance, unless it is impossible to obtain permission on time and any delay would present a risk. In this case the police shall, as soon as possible and within six hours of commencement of application of the measure at the latest, inform the state prosecutor, who may prohibit further application of the measure if he believes that there are no reasonable grounds for it. This measure may last for a maximum of 12 hours from contact with the person against whom the measure is being applied. When applying the measure from this paragraph, the police may not use technical equipment and devices from points 1 and 2 of the sixth paragraph of this article, nor may they apply the measure in private premises. The police shall make an official note immediately after the cessation of such surveillance and send it without delay to the state prosecutor that granted the permission from this paragraph and to the body that issued the original secret surveillance order. The official note shall become part of the criminal file.	
What ongoing supervision is required for the use of this tool?	Judicial supervision in cases when authorisation is given by the court or state prosecutor when they give authorisation. The measure of Surveillance is limited to 6 months after that the court have to approve extension for additional 6 month. After surveillance is finished the police has to report to state prosecutor and to the court in cases when approval was given by the court.	• ZKP (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362# • ZKP (English - not all changes and amendments are included) https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf
Is there any national case law relating to the use of this tool in cross-border crime cases?	We have found extensive case law for surveillance, however we could not identify cross-border cases. One case is described below. Case: VSK IV Kp 7664/2009 Casino H. filed a criminal complaint on 15 May 2007, according to the defense counsel for the convicted C., on suspicion that the "American roulette" game was not played in accordance with the rules at the table where the head P.J. and the player D.G. would cooperate and that D.C. is also said to have recently joined in doing so. In the present case, there was a suspicion of committing a criminal offense. A covert investigative measure of secret observation under the first paragraph of Article 149a of the ZKP has also begun. Data and evidence were collected in the direction of detecting and investigating the crime in question. The District Court in Nova Gorica found the convicted P. J. and D. C. guilty of complicity with Š. H. and S. Š. committed a continuing criminal offense of fraud under the second and first paragraphs of Article 217 in conjunction with Article 25 of the Criminal Code.	• Case: http://www.sodnapraksa.si/?q=149.a%20ZKP&database[SOVS]=SOVS&database[IESP]=IESP&database[VDSS]=VDSS&database[UPRS]=UPRS&database[SEU]=SEU&database[NEGM]=NEGM&database[SOSC]=SOSC&database[SOPM]=SOPM&submit=i%C5%A1%C4%8Di&rowsPerPage=20&page=0&id=2012032113063955
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Undercover / covert operations		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Procedure Act (ZKP), Official Gazette no. 32/12 – consolidated version, no. 47/13, 87/14, 8/16 – Constitutional Court decision, 64/16 – Constitutional Court decision, 65/16 – Constitutional Court decision, 66/17 – ORZKP153,154, 22/19, 55/20 - Constitutional Court decision, 89/20 - Constitutional Court decision, 191/20 - Constitutional Court decision and no. 200/20) Cooperation in Criminal Matters with the Member States of the European Union Act (ZSKZDČEU-1), Official Gazette of Republic of Slovenia no. 48/13, 37/15 in 22/18 Agreement between the Republic of Slovenia and the Republic of Austria on Police Cooperation (BATPS) Agreement between the Republic of Slovenia and the Republic of Hungary on cross-border co-operation of law enforcement authorities (BHUČPS)	• ZKP (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362# • ZKP (English - not all changes and amendments are included) https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf • Cooperation Act (Slovenian): http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6513 • Cooperation Act (English): https://www.ejtn.eu/PageFiles/6533/2014%20seminars/Nicosia/SI_Legislation/Law_Cooperation_Criminal_Matters.pdf

Relevant items	Provisions	Sources used
	Agreement between the Republic of Slovenia and the Republic of Italy on cross-border police cooperation (BITČPS) Agreement between the Republic of Slovenia and the Republic of Croatia on Cross-border police co-operation (BHRPS) Police Cooperation Convention for Southeast Europe (MKPS) (Official Gazette of Republic of Slovenia no. 18/12)	- BATPS (Slovenian & German): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2004-02-0052/#I.%C2%A0poglavjeSplo%C5%A1ne%C2%A0dolo%C4%8Dbe - BHUCPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0029?sop=2007-02-0029 - BITČPS (Slovenian & Italian): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0134?sop=2007-02-0134 - BHRPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2003-02-0014?sop=2003-02-0014 - MKPS (English) https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2012-02-0103/zakon-o-ratifikaciji-konvencije-o-policijskem-sodelovanju-v-jugovzhodni-evropi-mkps
How is the tool defined?	Article 155a in KZP (1) If there are reasonable grounds for suspecting that a certain person has committed any of the criminal offences from the fourth paragraph of Article 149a of this Act, or if it is reasonable to conclude that a certain person is involved in criminal activity connected with the criminal offences from the fourth paragraph of Article 149a of this Act and that other measures will not yield evidence or will give rise to disproportionate difficulties, undercover operations may be used against this person. (2) Undercover operations shall be carried out by undercover operatives and involve the continual gathering of information or repeat sessions of information gathering on a person and his criminal activities. Undercover operations shall be carried out by one or more undercover operatives under the direction and supervision of the police, using false information about an operative, false information in databases and false documents in order to prevent the information gathering process or the status of the operative from being disclosed. An undercover operative may be a police officer, a police employee of a foreign country or exceptionally, if undercover operations cannot be carried out in any other way, by another person. An undercover operative may, under conditions from this article, participate in legal transaction using false documents. When information is being gathered under the conditions from this article, technical devices for transmitting and recording sound, photography and video recording may also be used. There were special provisions on undercover operations in the Cooperation in Criminal Matters with the Member States of the European Union Act (ZSKZDČEU-1), Official Gazette of Republic of Slovenia no. 48/13, 37/15 in 22/18, which were annulled due to changes introduced by European Investigative Order, which is now covered by Article 77g and 77 h. Article 77.g: Issuance of a European investigation order for the purpose of carrying out covert operations (1) The competent investigating judge or public prosecutor may, in accordance with the law governing criminal proceedings, issue a European investigative order for the implementation of an investigative measure of secret operation with officials acting under a modified identity. (2) When issuing the European investigation order, the competent authority referred to in the preceding paragraph shall state why it considers that covert action will be important for an individual criminal proceeding. Article 77.h: Execution of a European investigation order for the purpose of conducting covert operations (1) A European investigative order for the performance of covert operations in the Republic of Slovenia shall be recognised and ordered to be executed by the public prosecutor or investigating judge competent for the area in which the covert operation is expected to begin, under the conditions and for the duration, which regulates criminal proceedings. (2) In addition to the reasons for refusing recognition and enforcement referred to in Article 62 of this Act, the European investigation order referred to in the preceding paragraph shall also be refused if the execution of the requested investigative measure would not be approved in a similar internal case. covert operations under the third paragraph of this Article. (3) Secret activities shall be carried out in accordance with the law governing criminal proceedings. The domestic authorities carrying out the European investigative order referred to in paragraph 1 of this Article shall have the exclusive right to direct and supervise covert operations. The duration of the covert operation, the conditions and the legal status of the officials involved in the covert operation shall be agreed directly by the domestic authorities with the issuing State. (4) An undercover officer of another Member State shall operate in the territory of the Republic of Slovenia under the direction and control of the police, to whom the order authorizing the undercover officer shall be sent with the designation "internally" in accordance with the law governing classified information. Bilateral agreements: Article 12 in BATPS	- ZKP (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362# - ZKP (English - not all changes and amendments are included) https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf - Cooperation in Criminal Matters Act (Slovenian): http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6513 - Cooperation in Criminal Matters Act (English): https://www.ejtn.eu/PageFiles/6533/2014%20seminars/Nicosia/SI_Legislation/Law_Cooperation_Criminal_Matters.pdf - BATPS (Slovenian & German): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2004-02-0052/#I.%C2%A0poglavjeSplo%C5%A1ne%C2%A0dolo%C4%8Dbe - BHUCPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0029?sop=2007-02-0029 - BITČPS (Slovenian & Italian): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0134?sop=2007-02-0134 - BHRPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2003-02-0014?sop=2003-02-0014 - MKPS (English) https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2012-02-0103/zakon-o-ratifikaciji-konvencije-o-policijskem-sodelovanju-v-jugovzhodni-evropi-mkps

Relevant items	Provisions	Sources used
	(1) Upon prior request by a Party, the other Party may authorize the clandestine operation of officials of the Requesting Party whose identity has been changed (undercover agents) in the territory of the Requesting Party if there are sufficient grounds to suspect that it is a criminal offense. , for which the operation of undercover workers is permitted under national law. The issued approval is valid for the entire territory of the country. The requesting Party shall transmit such a request only if the investigation of the facts without the planned investigative measures would be unsuccessful or substantially difficult. (2) Investigations in the territory of the requested Contracting Party shall be limited to individual, time-limited actions. Undercover operations may be granted for a period of up to one month, with the possibility of extension for a period of one month at a time. The preparation of such actions shall take place on the basis of close coordination between the participating authorities of the requested Party and the requesting Party. The official of the requested Contracting Party shall be responsible for conducting these operations. The actions of officials of the requesting Contracting Party shall be deemed to be those of the requested Contracting Party. At the request of the requested Party, investigations shall be terminated. (3) The conditions for the operation of undercover agents under which such undercover operation takes place and the possibility of using the results of the investigation shall be determined by the requested Contracting Party, taking into account its national law. The requested Contracting Party shall inform the requesting Contracting Party thereof. (4) The requested Contracting Party shall provide the necessary personnel, logistical and technical assistance and shall take all necessary measures to protect the officials of the requesting Contracting Party during their operation in the territory of the requested Contracting Party. (5) The request shall be addressed to the national central service or to the body responsible for issuing the approval, at the same time as the national central service is notified. The Contracting Parties shall exchange information on the authorities responsible for granting approval. (6) The competent authorities of the Contracting Party in whose territory they operated shall be notified in writing without delay of the performance and results of the activities of the undercover agents. (7) The Contracting Parties may exchange undercover agents acting on behalf of and under the direction of the competent authority of the requesting Contracting Party. Article 10 of BITCPS 1. Subject to the laws in force in both Contracting Parties and subject to prior detailed arrangements to be made between the competent authorities, the Contracting Parties undertake to facilitate and provide assistance in carrying out "controlled delivery" and the "covert operation". 2. The request referred from the previous paragraph must be sent: - in the Republic of Slovenia: the Ministry of the Interior, the Police, the General Police Administration, the Criminal Police Administration; - in the Italian Republic: the Ministry of the Interior, the Public Security Administration, the Central Directorate for the Fight against Drugs and for activities relating to investigations into drugs and psychotropic substances and precursors. The Central Directorate of the Criminal Police - International Police Cooperation Service is responsible for the remaining request. Article 16 in MKPS (1) In the course of investigations for criminal offences, a Contracting Party can, on the basis of a request received in advance, consent to the deployment of officers of the requesting Contracting Party under the terms of its legislation, who can play the role of an agent, or a person performing a controlled purchase (thereafter referred to as "undercover investigator"). The requesting Contracting Party shall make such a request only if the investigation of the criminal offence would otherwise be impossible or extremely impeded. The true identity of the officer need not be revealed in the request. (2) Undercover investigations on the territory of the requested Contracting Party shall be restricted to single, temporary operations. Preparations of these operations shall be done by way of coordination between the officers involved from the Contracting Parties. The deployment of an undercover investigator and the execution of the actions taken by the undercover investigator shall be managed by the requested Contracting Party. The requested Contracting Party is responsible for the action taken by an undercover investigator of the requesting Contracting Party, and can, at any time, demand the termination of the operation. (3) The deployment of undercover investigators under this Article, the conditions under which the operation is carried out and the terms for the use of the investigation results shall depend upon the legislation of that Contracting Party on whose territory the undercover investigator is deployed. (4) The requested Contracting Party shall grant the undercover investigator all necessary support in form of personnel, including the presence of his handler, logistics and technical equipment,	

Relevant items	Provisions	Sources used
	and shall take all necessary measures to protect the undercover investigator during the operation on its territory. (5) Due to extreme urgency, in case there is a serious danger that the identity of the undercover investigator can be revealed, the deployment of an undercover investigator on the territory of the other Contracting Party shall be admissible without prior consent as outlined in paragraph 1. In these cases, the preconditions for the deployment of the undercover investigator on the territory of the other Contracting Party must be met. The activities of the undercover investigator must be restricted to the extent absolutely essential for maintaining his/her cover story or his/her security. The requested Contracting Party shall be notified of the deployment without delay, and can, at any time, demand the termination of the operation. (6) Paragraphs 1 to 4 shall apply accordingly in cases where a Contracting Party requests the deployment of an undercover investigator of the other Contracting Party on its territory. In such cases, unless otherwise agreed upon, the requesting Contracting Party shall bear the costs of the operation. (7) The Contracting Parties shall take all necessary precautions to keep the undercover investigator's identity secret and to guarantee his/her security, also after his/her deployment is over.	
For what types of crime can the tool be used?	Article 155a in KZP (1) If there are reasonable grounds for suspecting that a certain person has committed any of the criminal offences from the fourth paragraph of Article 149a of this Act, or if it is reasonable to conclude that a certain person is involved in criminal activity connected with the criminal offences from the fourth paragraph of Article 149a of this Act and that other measures will not yield evidence or will give rise to disproportionate difficulties, undercover operations may be used against this person. Article 149a in connection to Article 155a in KZP (4) The criminal offences for which secret surveillance may be ordered are as follows: 1) criminal offences for which the law prescribes a prison sentence of five or more years; 2) criminal offences from point 2 of the second paragraph of Article 150 of this Act and the criminal offences of false imprisonment (Article 143 of the Penal Code), threatening the safety of another person (Article 145), fraud (Article 217), concealment (Article 221), disclosure of and unauthorised access to trade secrets (Article 241), abuse of inside information (Article 243), fabrication and use of counterfeit stamps of value or securities (Article 250), forgery (Article 256), special cases of forgery (Article 257), abuse of office or official rights (Article 261), disclosure of an official secret (Article 266), being an accessory after the fact (Article 287), endangering the public (Article 317), pollution and destruction of the environment (Article 333), bringing of hazardous substances into the country (Article 335), pollution of drinking water (Article 337), and tainting of foodstuffs or fodder (Article 338)	• ZKP (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362# • ZKP (English - not all changes and amendments are included) https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf
Does national law allow this tool to be used in cross border cases?	YES, Criminal procedure act is not specific about it, but the tool is part of bilateral agreements. The tool is covered by European Investigative order in terms of cooperation in criminal matters.	
What thresholds must be passed for the use of this tool?	In principle for criminal offence for which prison sentence of 5 or more years is prescribed, other criminal offences are specifically listed. Article 155a in KZP (1) If there are reasonable grounds for suspecting that a certain person has committed any of the criminal offences from the fourth paragraph of Article 149a of this Act, or if it is reasonable to conclude that a certain person is involved in criminal activity connected with the criminal offences from the fourth paragraph of Article 149a of this Act and that other measures will not yield evidence or will give rise to disproportionate difficulties, undercover operations may be used against this person. Article 149a in connection to Article 155a in KZP (4) The criminal offences for which secret surveillance may be ordered are as follows: 1) criminal offences for which the law prescribes a prison sentence of five or more years; 2) criminal offences from point 2 of the second paragraph of Article 150 of this Act and the criminal offences of false imprisonment (Article 143 of the Penal Code), threatening the safety of another person (Article 145), fraud (Article 217), concealment (Article 221), disclosure of and unauthorised access to trade secrets (Article 241), abuse of inside information (Article 243), fabrication and use of counterfeit stamps of value or securities (Article 250), forgery (Article 256), special cases of forgery (Article 257), abuse of office or official rights (Article 261), disclosure of an official secret (Article 266), being an accessory after the fact (Article 287), endangering the public (Article 317), pollution and destruction of the environment (Article 333), bringing of hazardous substances into the country (Article 335), pollution of drinking water (Article 337), and tainting of foodstuffs or fodder (Article 338)	• ZKP (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362# • ZKP (English - not all changes and amendments are included) https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf

Relevant items	Provisions	Sources used
What types of stakeholder are involved in the implementation of this tool?	The stakeholders are the police, state prosecutor and. court (investigative judge). Undercover officer can be police officer of Slovenia, police officer of foreign country, or in exceptional cases informed. (Article 155.a (2))	• ZKP (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362# • ZKP (English - not all changes and amendments are included) https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf
Which LEAs can use this tool?	Police	
	Article 155a in KZP (2) Undercover operations shall be carried out by undercover operatives and involve the continual gathering of information or repeat sessions of information gathering on a person and his criminal activities. Undercover operations shall be carried out by one or more undercover operatives under the direction and supervision of the police, using false information about an operative, false information in databases and false documents in order to prevent the information gathering process or the status of the operative from being disclosed. An undercover operative may be a police officer, a police employee of a foreign country or exceptionally, if undercover operations cannot be carried out in any other way, by another person. An undercover operative may, under conditions from this article, participate in legal transaction using false documents. When information is being gathered under the conditions from this article, technical devices for transmitting and recording sound, photography and video recording may also be used. Article 12 in BATPS (3) The conditions for the operation of undercover agents under which such undercover operation takes place and the possibility of using the results of the investigation shall be determined by the requested Contracting Party, taking into account its national law. The requested Contracting Party shall inform the requesting Contracting Party thereof. Secretariat for MKPS prepared a manual for execution of the convention: 6.4. Normal or ordinary undercover investigation in the territory of the requesting Contracting Party - A Contracting Party can request the deployment of an undercover investigator of the other Contracting Party in its territory. - The provisions of chapter 6.2. of the PCC Manual shall apply accordingly. - Unless otherwise agreed, the costs of such an operation shall be covered by the requesting Contracting Party. 6.5. Urgent or emergency undercover operation - Prior approval could not be obtained because the case was extremely urgent. This applies to the cases in which there is a serious danger that the identity of the undercover investigator can be revealed. - A criminal investigation must have started. - Only officers are allowed to carry out undercover investigations. - The border-crossing is without delay reported to the central national unit in the requested State. - The activities of the undercover investigator are restricted to the extent absolutely essential for maintaining his/her cover story or his/her security. - A request is submitted without any delay. An urgent reply is necessary from the requested State as to whether the request is approved or rejected. - The requested Contracting Party can, at any time, demand the termination of the operation. 6.6. Undercover investigations to prevent criminal offences - Upon request of a Contracting Party and as far as permissible under the respective national legislation, undercover investigations to prevent extraditable crimes can be carried out in the territory of the other Contracting Party, if consent has been given to this cross-border undercover investigation. - The provisions of chapter 6.1. - 6.5. of the PCC Manual shall apply accordingly.	• ZKP (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362# • ZKP (English - not all changes and amendments are included) https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Paragraph 6 of Article 155a - time limit (6) Application of the measure may last a maximum of two months. If due cause is adduced, it may be extended every two months by means of a written order, but to a maximum of 24 months. In the case of the use of a measure for criminal offences from the second paragraph of Article 151 of this Act, the maximum duration shall be 36 months. Monthly reporting of the police to the state prosecutor and the court in cases of extension	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Article 155a in KZP (3) An undercover operation measure shall be permitted by the state prosecutor on the basis of a written order and at the written request of the police, except in cases from the fourth paragraph of this article, where the order must be issued by the investigating judge. The order may also encompass permission to manufacture, obtain and use false information and documents. (4) An undercover operation measure where the undercover police employee will use technical devices for transmitting and recording sound, photography and video recording may only be ordered in connection with criminal offences from the second paragraph of Article 150 of this Act.	• ZKP (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362# • ZKP (English - not all changes and amendments are included) https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf

Relevant items	Provisions	Sources used
	The measure shall be ordered by the investigating judge in writing, at the written request of the state prosecutor. Article 150 in KZP in connection to Article 155a (4) (2) The criminal offences in connection with which the measures from the previous paragraph may be ordered are: 1) criminal offences against the security of the Republic of Slovenia and its constitutional order, and crimes against humanity and international Act for which the law prescribes a prison sentence of five or more years; 2) the criminal offence of kidnapping under Article 144, the showing, possession, manufacture and distribution of pornographic material under Article 187, illegal production of and trade in drugs under Article 196, enabling the taking of drugs under Article 197, blackmail under Article 218, abuse of inside information under Article 243, unlawful acceptance of gifts under Article 247, unauthorised giving of gifts under Article 248, money laundering under Article 252, smuggling under Article 255, accepting of a bribe under Article 267, giving of a bribe under Article 268, acceptance of gifts to secure unlawful intervention under Article 269, giving of gifts to secure unlawful intervention under Article 269a, criminal association under Article 297, illegal manufacture of and trade in arms or explosives under Article 310, and causing danger with nuclear substances under Article 319 of the Penal Code of the Republic of Slovenia; 3) other criminal offences for which the law prescribes a prison sentence of eight or more years.	
What ongoing supervision is required for the use of this tool?	Article 155a in KZP (2).. Undercover operations shall be carried out by one or more undercover operatives under the direction and supervision of the police, using false information about an operative, false information in databases and false documents in order to prevent the information gathering process or the status of the operative from being disclosed. An undercover operative may be a police officer, a police employee of a foreign country or exceptionally, if undercover operations cannot be carried out in any other way, by another person.. Article 155a in KZP (7) The provisions of the eleventh and twelfth paragraphs of Article 149a of this Act shall be applied mutatis mutandis to the cessation of application of undercover operations, the compilation of monthly reports by the police and the review of extension by the panel (sixth paragraph of Article 25). Article 149a in KZP in connection to Article 155a KZP (12) If a measure is applied against the same person for more than six months, the panel (sixth paragraph of Article 25) shall review the legality of and grounds for application of the measure upon the first extension over six months and every further six months thereafter. The body that issued the extension order shall send the panel all the relevant material; the panel shall decide within three days. If the panel assesses that there are no grounds for application of the measure or that all the legal conditions have not been fulfilled, it shall issue a decision ordering that the measure come to an end. There shall be no appeal against this decision. Article 25, sixth paragraph in connection to Article 155a (6) Circuit courts shall, in panels of three judges, hear appeals against rulings by examining magistrates of circuit courts, appeals against decisions passed by individual judges of district courts in their conducting of acts of investigation, and appeals against other decisions if so provided by this Act; rule in first instance outside the main hearing; conduct proceedings and pass judgements under the provisions of Article 517 of this Act; propose motions in cases provided by this Act or some other law.	• ZKP (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362# • ZKP (English - not all changes and amendments are included) https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf
Is there any national case law relating to the use of this tool in cross-border crime cases?	We did not find international case for tool Undercover. Case: VSM II Kp 47810/2010 In this case, the report of the Austrian security authorities was basis for order of undercover operations by the state prosecutor. The accused appealed the case on the grounds that the source of information is not identified and cannot present grounds for order of undercover operations. The court rejected the case on the merits that information from foreign authorities is not the same as information from anonymous source.	• http://www.sodnapraksa.si/?q=155.a%20ZKP%20avstrij*&database[SOVS]=SOVS&database[IESP]=IESP&database[VDSS]=VDSS&database[UPRS]=UPRS&database[SEU]=SEU&database[NEGM]=NEGM&database[SOSC]=SOSC&database[SOPM]=SOPM&submit=i%C5%A1%C4%8Di&rowsPerPage=20&page=0&id=2012032113063775
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	We have reviewed annual police and state prosecutes reports but we have not find any relevant data to the tool.	
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Procedure Act (ZKP), Official Gazette no. 32/12 – consolidated version, no. 47/13, 87/14, 8/16 – Constitutional Court decision, 64/16 – Constitutional Court decision, 65/16 – Constitutional Court decision, 66/17 – ORZKP153,154, 22/19, 55/20 - Constitutional Court decision, 89/20 - Constitutional Court decision, 191/20 - Constitutional Court decision and no. 200/20)	• ZKP (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362# • ZKP (English - not all changes and amendments are included) https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf

Relevant items	Provisions	Sources used
	Cooperation in Criminal Matters with the Member States of the European Union Act (ZSKZDČEU-1), Official Gazette of Republic of Slovenia no. 48/13, 37/15 in 22/18 Agreement between the Republic of Slovenia and the Republic of Austria on Police Cooperation (BATPS) Agreement between the Republic of Slovenia and the Republic of Hungary on cross-border co-operation of law enforcement authorities (BHUČPS) Agreement between the Republic of Slovenia and the Republic of Italy on cross-border police cooperation (BITČPS) Agreement between the Republic of Slovenia and the Republic of Croatia on Cross-border police co-operation (BHRPS) Police Cooperation Convention for Southeast Europe (Official Gazette of Republic of Slovenia no. 18/12) (MKPS) Police Tasks And Powers Act (Official Gazette of Republic of Slovenia no. 15/13, 23/15 – popr., 10/17, 46/19 – odl. US in 47/19) (ZNPPol) Organisation and Work of the Police Act (ZODPol) Official Gazette of the Republic of Slovenia no. 15/13, 11/14, 86/15, 77/16, 77/17, 36/19, 66/19 – ZDZ in 200/20	- Cooperation Act (Slovenian): http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6513 - Cooperation Act (English): https://www.ejtn.eu/PageFiles/6533/2014%20seminars/Nicosia/SI_Legislation/Law_Cooperation_Criminal_Matters.pdf - BATPS (Slovenian & German): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2004-02-0052/#I.%C2%A0poglavjeSplo%C5%A1ne%C2%A0dolo%C4%8Dbe - BHUČPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0029?sop=2007-02-0029 - BITČPS (Slovenian & Italian): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0134?sop=2007-02-0134 - BHRPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2003-02-0014?sop=2003-02-0014 - MKPS (English) https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2012-02-0103/zakon-o-ratifikaciji-konvencije-o-policijskem-sodelovanju-v-jugovzhodni-evropi-mkps - ZNPPol (Slovenian) http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6314 - ZODPol (Slovenian) http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6315
Specific range of application of the tool	General provisions on gathering information at any indication of criminal offence according to Article 148 of The Criminal Procedure Act refers to general public as well as Article 11 of Police Tasks And Powers Act which is referring to criminal intelligence gathering. The legislation does not specify but informants can also witnesses to crimes, victims of crime or members of OCG.	
How is the tool defined?	Article 148 in ZKP (1) If grounds exist for suspicion that a criminal offence liable to public prosecution has been committed, the police shall be bound to take steps necessary for discovering the perpetrator, ensuring that the perpetrator or his accomplice do not go into hiding or flee, detecting and preserving traces of crime or objects of value as evidence, and collecting all information that may be useful for the successful conducting of criminal proceedings. (2) With a view to executing the tasks from the preceding paragraph the police may: seek information from citizens. Registered informants are considered as individuals offering assistance to the police. According to Article 33 of the Organisation and Work of the Police Act (ZODPol) such individuals enjoy certain rights. (1) An individual who voluntarily and with the consent of a police officer assists in the performance of police tasks specified by law and is injured or loses his or her ability to work is entitled to all rights and benefits arising from health, pension and disability insurance. eligible police officer in case of injury at work. (2) The basis for the assessment of the rights referred to in the preceding paragraph shall be the basic salary of a police officer in the lowest salary grade or the individual's salary, if this is more favourable for him. (3) If an individual loses his life while assisting the police, his family members shall be entitled to a survivor's pension in accordance with the law governing pension and disability insurance. (4) Close family members (spouse, common-law partner, partner from a registered same-sex partnership, children and adopted children) of the individual referred to in the previous paragraph are jointly entitled to a one-time financial assistance in the amount of the last six monthly salaries of that individual. salary grade, if this is more favourable for them. (5) An individual who has assisted the police has the right to compensation for the damage he or she has received as a result of the assistance provided. (6) In the event of endangerment of an individual who has assisted or is assisting the police and his relatives, the police may carry out the measures specified in Article 66 of this Act (<i>i.e. protection - added by EY</i>). The written consent of the endangered person is required for the implementation of the measures. (7) Under this Act, close family members and other persons who are in a confidential relationship with an individual and who are at least likely to prove this circumstance shall be considered close. (8) If pre-trial, criminal or civil proceedings are instituted against an individual who assisted the police in connection with the given assistance, the police shall provide him with paid legal assistance in these proceedings in the manner specified in the regulation referred to in Article 64 of this Act. Article 17 in BHUČPS 1. In accordance with requests received via their central contact points, the authorised co-operating authorities of the Contracting Parties may, in the course of crime detection and in accordance with the internal laws and regulations of their states, covertly gather information and inform each other of the results.	- ZKP (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362# - ZKP (English - not all changes and amendments are included) https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf - Cooperation Act (Slovenian): http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6513 - Cooperation Act (English): https://www.ejtn.eu/PageFiles/6533/2014%20seminars/Nicosia/SI_Legislation/Law_Cooperation_Criminal_Matters.pdf - BATPS (Slovenian & German): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2004-02-0052/#I.%C2%A0poglavjeSplo%C5%A1ne%C2%A0dolo%C4%8Dbe - BHUČPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0029?sop=2007-02-0029 - BITČPS (Slovenian & Italian): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2007-02-0134?sop=2007-02-0134 - BHRPS (Slovenian & English): https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2003-02-0014?sop=2003-02-0014 - MKPS (English) https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2012-02-0103/zakon-o-ratifikaciji-konvencije-o-policijskem-sodelovanju-v-jugovzhodni-evropi-mkps - ZNPPol (Slovenian) http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6314 - ZODPol (Slovenian) http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO6315

Relevant items	Provisions	Sources used
	2. In addition to the data set forth in Article 4 (1) of this Agreement, the request for covert gathering of information shall include: a) indication of the instrument or method; b) the duration of the covert measure; c) the scope of data to be recorded and transferred; d) the manner of transferring the data; e) the manner of providing assistance in the event of the covert gathering of information in the other country; f) a copy of the authorisation by the authority in charge of the covert gathering of information related to the detection of a criminal act in progress in the state of the requesting Contracting Party. 3. To the extent that the national laws and regulations of the Contracting Parties require the authorisation of the judicial authorities for compliance with a request for the covert gathering of information, a copy of the authorisation shall be sent to the requested Contracting Party. If no such authorisation is required the requesting Contracting Party shall inform the central contact point of the requested Contracting Party thereof in the request. The authorised co-operating authority of the requested Contracting Party shall begin processing the request in accordance with its national laws and regulations and, when needed, after obtaining the authorisation from its judicial authority. 4. The Contracting Parties undertake to grant at least the same level of protection to the person co-operating with the law enforcement authorities and the data provided by him as that stipulated by the laws and regulations of their states for the protection of persons co-operating with their law enforcement authorities and the data provided by them. Article 11 in ZNPPol (1) Criminological acquisition and evaluation of information shall be a process of collecting, evaluating and analysing personal and other data on criminal activities of natural persons and legal entities and criminal organisations that facilitate the decision-making and planning related to police tasks aimed at prevention, detection and investigation of criminal offences, the perpetrators of which are prosecuted ex officio. (2) In acquiring data referred to in the preceding paragraph, the police shall cooperate with persons who voluntarily provide the police with operational information about criminal offences, their perpetrators and other activities suggesting elements of criminal offences. (3) Criminological acquisition and evaluation of information may not incite criminal activities. (4) The police shall ensure persons referred to in paragraph two of this Article safety and anonymity if this is in their interest and in accordance with the provision of Article 118 of this Act. (5) The method of criminological acquisition and evaluation of information and cooperation with persons shall be determined by the Director General of the Police through an internal act. Article 5 in MKPS (1) In the course of cooperation aiming at preventing, detecting and investigating criminal offences, in particular organised crime, the law enforcement authorities of the Contracting Parties shall, upon request, exchange the following information: a) on data of individuals involved in organised crime, intelligence on links between the suspects and persons under suspicion in relation to commission of criminal offences, their knowledge on the structure of criminal organisations and groups, and about typical behaviour patterns of suspects and persons under suspicion or suspect groups and groups under suspicion, information on prepared, attempted, or accomplished criminal offences, especially time, scene and type of crime, details on victims or victimised property, intelligence on the particular circumstances and about the relevant legal provisions, if required to prevent, detect and investigate criminal offences, b) on methods and new forms of transborder crime, c) on criminological and other crime-related research results, details on practice of conducting investigations, working means and methods aiming at their further development, d) on intelligence and/or samples of items or property that were damaged during the crime, or were used or intended to commit a crime or which were the result of a committed crime, e) on legislation in force relating to the crimes that are subject of this Convention, f) on criminal proceeds and assets acquired through commission of or involvement in crime. (2) When obtaining information by means of special methods, the authorities of the Contracting Parties shall cooperate in compliance with their national legislation. The Contracting Parties undertake to ensure at least the same standard of protection for data transmitted in the course of such information exchange as prescribed by the respective national legal provisions.	
For what types of crime can the tool be used?	Cross crime areas no limitations on types of SOC.	
Does national law allow this tool to be used in cross border cases?	National legislation is not specific about use of informants in cross border criminal investigations. However, information obtained from informants is exchanged in such cases. There is also no	

Relevant items	Provisions	Sources used
	limitations on use of informant from any other country on the national territory. There can be some overlap between tool, since undercover police officers use informants as method of work (see other tools).	
What thresholds must be passed for the use of this tool?	Article 148 in ZKP (1) If grounds exist for suspicion that a criminal offence liable to public prosecution has been committed, the police shall be bound to take steps necessary for discovering the perpetrator, ensuring that the perpetrator or his accomplice do not go into hiding or flee, detecting and preserving traces of crime or objects of value as evidence, and collecting all information that may be useful for the successful conducting of criminal proceedings.	• ZKP (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362# • ZKP (English - not all changes and amendments are included) https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf
What types of stakeholder are involved in the implementation of this tool?	Police	
Which LEAs can use this tool?	Police	
What are the rules to be followed for the implementation of this tool?	<i>All human sources which are given status of informant have to be registered according to the internal rules of the police.</i> <i>Identity of informant has to be protected and confidential.</i>	• ZKP (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362# • ZKP (English - not all changes and amendments are included) https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	No specific restrictions.	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	No authorisation is required to use informant. Authorisation would be required if informant would be used as undercover officer, which is possible under article 149a of the Criminal procedure Code, but in such case order by the investigative judge upon written request of the state prosecutor would be required. However, this is only in exceptional cases. Article 17 in BHUČPS 3. To the extent that the national laws and regulations of the Contracting Parties require the authorisation of the judicial authorities for compliance with a request for the covert gathering of information, a copy of the authorisation shall be sent to the requested Contracting Party. If no such authorisation is required the requesting Contracting Party shall inform the central contact point of the requested Contracting Party thereof in the request. The authorised co-operating authority of the requested Contracting Party shall begin processing the request in accordance with its national laws and regulations and, when needed, after obtaining the authorisation from its judicial authority.	
What ongoing supervision is required for the use of this tool?	Police supervision. Rules and guidelines of the Police on work with informants are confidential.	• ZKP (Slovenian): http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO362# • ZKP (English - not all changes and amendments are included) https://www.policija.si/images/stories/Legislation/pdf/CriminalProcedureAct2007.pdf
Is there any national case law relating to the use of this tool in cross-border crime cases?	Information provided by the informants are in most case treated as intelligence to assist and guide police work. Informants are in principle not called as witnesses. In cases where this is necessary, their identity can be kept secret. The Constitutional Court in case no. Up-754/04-14 on 14th 9. 2006 reached a Decision on annulment of judgments of the Supreme Court, the High Court in Maribor and the District Court in Maribor. In the case accused was not allowed to examine the undercover police officer who was directly involved in sale of drugs. The court decided that this is violation of rights of accused. However, it emphasised that there are many option in place to protect identity of police officer (i.e. his personal information is not disclosed). In case of witnesses protection can be even more extensive (i.e. deletion of certain data from the criminal file, marking of certain data for official secrecy, determination of the pseudonym of the witness, interrogation by means of technical means, such as a firewall, voice distortion device, transmission of sound from a special room, etc.). In case that informant was witness to the criminal offence such measures would be taken.	• Court decision (Slovenian): http://www.pisrs.si/Pis.web/pregledPredpisa?id=ODLU1007
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	

Source: Author's own elaboration

Slovakia

Table 45 – Overview of national rules on investigative tools - Slovakia

Relevant items	Provisions	Sources used
Controlled Delivery		

Relevant items	Provisions	Sources used
Relevant documents (legal and non-legal) that define the functioning of the tool	Code of Criminal Procedure 301/2005 Coll. Article 111 Act on Police Force 171/1993 Coll. Article 39 Act on Financial Administration 35/2019 Coll. Article 16	https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2005/301/20160101.html
How is the tool defined?	Controlled delivery means the monitoring of the movement of the consignment from the sender to the addressee during its transit, export or import, if the circumstances of the case justify the assumption that the consignment without the necessary permits contains narcotic substances, psychotropic substances, precursors, poisons, nuclear or other radioactive materials, hazardous chemical substances, counterfeit or altered money, counterfeit or altered securities, counterfeit, altered or illegally produced custom stamps, postal stamps, labels and postal stamps, electronic means of payment or another payment card or an item capable of such function, firearms or weapons of mass destruction, ammunition and explosives, cultural heritage items or other items that require special permissions for their possession, items intended to commit a criminal offence, or items of a committed criminal offence, for the purpose of apprehending persons who take part in the handling of such consignment.	- Code of Criminal Procedure 301/2005 Coll. - Article 111 (paragraph 1)
For what types of crime can the tool be used?	Tool can be used for consignments containing drugs, psychotropic substances, poisons, precursors, nuclear or other similar radioactive material, or high-risk chemical, counterfeit or altered money and counterfeit or altered securities, counterfeit, altered or illicitly produced stamps, postage stamps, stickers and postage stamps, electronic means of payment or other payment card, or an object capable of performing such a function, firearm or collectively effective weapons, ammunition and explosives, cultural monuments or other items for which a special permit is required.	- Code of Criminal Procedure 301/2005 Coll. - Article 111 (paragraph 1)
Does national law allow this tool to be used in cross border cases?	Tool can be used for both national and cross border investigations; cross border use requires an international legal assistance request or cooperation within a Joint Investigation Team	- Code of Criminal Procedure 301/2005 Coll. - Article 531 - 540
What thresholds must be passed for the use of this tool?	No thresholds are identified in the national law provisions or legal norms.	N/A
What types of stakeholder are involved in the implementation of this tool?	Judicial authorities - presiding judge approves the request of the respective LEA (Police Force or Criminal Office of the Financial Administration) and issues the warrant to execute controlled delivery in cases when criminal proceedings have been already commenced. Prosecutor approves the request of the respective LEA (Police Force or Criminal Office of the Financial Administration) and issues the warrant to execute controlled delivery in cases prior the commencement of criminal proceedings or in the preparatory proceedings. LEA (Police Force and Criminal Office of the Financial Administration) - appointed LEA officer (investigator) issues a requests for controlled delivery to be approved either by the presiding judge or the prosecutor (depending whether the criminal proceedings have been already commenced). If the request is approved and the warrant issued, LEA officers execute the controlled delivery	- Code of Criminal Procedure 301/2005 Coll. - Article 111 (paragraph 2 & 3)
Which LEAs can use this tool?	Police Force and Criminal Office of the Financial Administration respectively to their competencies according to the Code of the Criminal Procedure.	- Code of Criminal Procedure 301/2005 Coll. - Article 111 (paragraph 3) - Act on Police Force 171/1993 Coll. - Article 39 - Act on Financial Administration 35/2019 Coll. - Article 16 - N/A
What are the rules to be followed for the implementation of this tool?	Legal obligations and requirements are indicated in respective fields in this section. Detailed rules for the implementation of the tool are restricted for Personnel of the respective units and are not publicly available.	N/A
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Tool can be used in the criminal procedure only with a warrant issued by a judge. Please refer to question regarding the authorisation needed for the use of this tool.	- Code of Criminal Procedure 301/2005 Coll. - Article 111 (paragraph 2 & 4)
What authorisation is needed for the use of this tool?	The warrant for the controlled delivery shall be issued by the presiding judge; before the commencement of criminal proceedings or in the preparatory proceedings by the prosecutor. The Police Force may commence the monitoring of the consignment without the warrant if the case cannot be deferred and the warrant cannot be procured in advance. The Police Force shall notify the public prosecutor of such act without undue delay. If the public prosecutor fails to issue a warrant within 48 hours, the monitoring of the consignment must be terminated and the obtained information can no longer be used in further proceedings and must be destroyed in the prescribed manner without undue delay.	- Code of Criminal Procedure 301/2005 Coll. - Article 111 (paragraph 2 & 4)
What ongoing supervision is required for the use of this tool?	No ongoing supervision is required by the national law	- Code of Criminal Procedure 301/2005 Coll. - Article 111 (paragraph 2)
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	N/A

Relevant items	Provisions	Sources used
Data available on the number of times this tool has been used for SOC cases	N/A	
Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	Schengen Agreement Article 41 Bilateral agreements on cross-border police cooperation with HU, AT, CZ and PL. Act on the Police Force 171/1993 Coll. Article 77b, 77c Act on Financial Administration 35/2019 Coll. Article 51	• https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A42000A0922%2802%29 • https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1993/171/20200101 • https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2019/35/20210301
How is the tool defined?	Officers of one of the Contracting Parties who are pursuing in their country an individual caught in the act of committing or of participating in one of the offences referred to in paragraph 4 shall be authorised to continue pursuit in the territory of another Contracting Party without the latter's prior authorisation where, given the particular urgency of the situation, it is not possible to notify the competent authorities of the other Contracting Party by one of the means provided for in Article 44 prior to entry into that territory or where these authorities are unable to reach the scene in time to take over the pursuit.	• Schengen Agreement • Article 41 (paragraph 1)
For what types of crime can the tool be used?	(a) The following criminal offences: murder, manslaughter, rape, arson, forgery of money, aggravated burglary and robbery and receiving stolen goods, extortion, kidnapping and hostage taking, trafficking in human beings, illicit trafficking in narcotic drugs and psychotropic substances, breach of the laws on arms and explosives, wilful damage through the use of explosives, illicit transportation of toxic and hazardous waste, failure to stop and give particulars after an accident which has resulted in death or serious injury. (b) Extraditable offences.	• Schengen Agreement • Article 41 (paragraph 4 a/b)
Does national law allow this tool to be used in cross border cases?	National law does not cover this particular tool within its legislation. Hot Pursuit is covered within the Schengen Agreement and Bilateral cross-border cooperation agreements with neighbouring EU / Schengen member states.	
What thresholds must be passed for the use of this tool?	No thresholds are identified in national law provisions or legal norms.	• Schengen Agreement • Article 41
What types of stakeholder are involved in the implementation of this tool?	The pursuing officers shall, not later than when they cross the border, contact the competent authorities of the Contracting Party in whose territory the hot pursuit is to take place.	• Schengen Agreement • Article 41 (section 3)
Which LEAs can use this tool?	Police Force and Criminal Office of the Financial Administration There is no specific mention of this mechanism in the criminal procedure code, just a general reference in section 77b and 77c of the Police force act and section 51 of the Act on Financial Administration, stipulating that a member of the Slovak police force / Financial Administration could carry out hot pursuit on the territory of another state on the basis of an international treaty. The same regulation is valid also for police officers from other countries to carry out their powers on the territory of Slovakia.	• Act on the Police Force 171/1993 Coll. • Article 77b and 77c • Act on Financial Administration 35/2019 Coll. • Article 51
What are the rules to be followed for the implementation of this tool?	Legal obligations and requirements are indicated in respective fields in this section. Detailed rules for the implementation of the tool are restricted for Personnel of the respective units and are not publicly available.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Respective provisions of Schengen Agreement and Bilateral cross-border agreements outlined below in the question regarding the authorisation needed for the use of this tool must be met.	• Schengen Agreement • Article 41 (section 3)
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	The pursuing officers shall, not later than when they cross the border, contact the competent authorities of the Contracting Party in whose territory the hot pursuit is to take place. The hot pursuit will cease as soon as the Contracting Party in whose territory the pursuit is taking place so requests. At the request of the pursuing officers, the competent local authorities shall challenge the pursued person in order to establish the person's identity or to make an arrest.	• Schengen Agreement • Article 41 (section 3)
What ongoing supervision is required for the use of this tool?	Tool does not require judicial supervision. Rules given by the Schengen Agreement and respective Bilateral Agreements need to be followed. Internal approval within the Police Force and Financial Administration are subject to respective internal rules and regulation and are not publicly available.	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	Code of Criminal Procedure 301/2005 Coll. Article 136,137, 138 and 139 Act on Witness Protection and on Amendments to Certain Acts 256/1998 Coll.	• https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2005/301/ • https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1998/256/20160101

Relevant items	Provisions	Sources used
How is the tool defined?	Criminal procedure code contains specific regulation regarding witness protection and recognises three different degrees of protection: first by not stating the place of residence, second –removal of all personal data of a witness from the case and third by entering into the witness protection programme. Act on witness protection regulates conditions and procedures for granting protection to endangered witnesses. One of the main conditions for witness protection is witness` adherence to rules set out in the protection agreement.	• Code of Criminal Procedure 301/2005 Coll. • Article 136,137, 138 and 139 • Act on Witness Protection and on Amendments to Certain Acts 256/1998 Coll. • Article 1 (paragraph 1)
For what types of crime can the tool be used?	National law explicitly do not provide information about what crime needs to be committed, for this tool to be applicable. Professional judgement is exercised case by case.	• N/A
Does national law allow this tool to be used in cross border cases?	Tool can be used for both national and cross border investigations	• Act on Witness Protection and on Amendments to Certain Acts 256/1998 Coll. • Article 11 (paragraph 1, 2)
What thresholds must be passed for the use of this tool?	Due no specification of crimes are listed in the National law provisions, there are no thresholds mentioned for witness protection tool.	• N/A
What types of stakeholder are involved in the implementation of this tool?	Judicial authorities - presiding judge prepares and files a request for the witness protection in the case when court proceedings have been already commenced. Public prosecutor, or a police investigator with prosecutor's written approval, prepares and files the request for the witness protection during the preparatory proceedings. Commission deciding upon merits of the above requests, consisting of a Chairperson and four members. Chairperson and one of the members, and their deputies are appointed and removed by the Minister of the Interior of the Slovak Republic from among the members of the Police Force. The two members of the commission and their deputies are appointed and by the Minister of Justice of the Slovak Republic from subordinate employees with experience in the judiciary and imprisonment matters, and one member and his deputy are appointed by the Prosecutor General of the Slovak Republic from the prosecutors of the General Prosecutor's Office of the Slovak Republic. Police Force - specialised Witness Protection Unit is responsible for execution of the protective measures including the identity change etc.	• Act on Witness Protection and on Amendments to Certain Acts 256/1998 Coll. • Article 2 (paragraph 1) • Article 3 (paragraph 1) • Article 4 (paragraph 2)
Which LEAs can use this tool?	Police Force - Witness Protection Unit	• Act on Witness Protection and on Amendments to Certain Acts 256/1998 Coll. • Article 2 (paragraph 2)
What are the rules to be followed for the implementation of this tool?	Legal obligations and requirements are indicated in respective fields in this section. Detailed rules for the implementation of the tool are restricted for Personnel of the respective units and are not publicly available.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Request of respective judicial authority and approval of a special Commission is required. Please refer to question regarding the authorisation needed for the use of this tool.	• Act on Witness Protection and on Amendments to Certain Acts 256/1998 Coll. • Article 3 (paragraph 1 - 3) • Article 5 (paragraph 1 and 2)
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	The request, prepared and filed by respective judicial authority shall be submitted to the Witness Protection Unit of the Police Force. Unit shall immediately forward the request to the chairman of the Commission, who shall ensure that a meeting is held no later than seven days from the date of its receipt. At the meeting, the commission decides by vote on the proposal and respective measures. Justification of the proposal for measures should include, in particular, a description of the criminal case in which the endangered witness testifies and the nature of the danger threatening the endangered witness. If the matter cannot be deferred, the chairperson of the Commission or, in their absence, their deputy shall immediately decide on the proposal for measures in writing. If the decision of the chairperson of the Commission (or, in his absence his deputy's) is positive (i.e. request is approved), they shall inform the other members of the commission.	• Act on Witness Protection and on Amendments to Certain Acts 256/1998 Coll. • Article 3 (paragraph 1 - 3) • Article 5 (paragraph 1 and 2)
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Surveillance		
Relevant documents (legal and non-legal) that define the functioning of the tool	Code of the Criminal Procedure 301/2005 Coll. Article 113, 114, 115 Act on Police Force 171/1993 Coll. Article 36, 39 Act on Financial Administration 35/2019 Coll. Article 14, 16	• https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2005/301/ • https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2019/35/ • https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2003/166/20160101 • https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2003/166/20160101

Relevant items	Provisions	Sources used
	Act No. 166/2003 on Protection against Unlawful Use of Information and Technical Means (Wiretapping Protection Act).	
Specific range of application of the tool	National legislation specifically mentions following types of activities: - Physical surveillance (observation) - Audio and video recording - Interception and recording of telecommunication operations Activities defined in the legislation are however understood in a broader concept and allow also using various techniques and devices including GPS transponders, body worn devices, listening devices etc., although they are not explicitly mentioned in the legislation. Interception and recording of telecommunication traffic may also include data surveillance and other techniques.	• Code of Criminal Procedure 301/2005 Coll. • Article 113, 114, 115
How is the tool defined?	The surveillance of persons and items means acquiring information on the movements and activities of persons or the movement of items that is performed in a classified manner; surveillance may be performed in the criminal proceedings on an intentional criminal offence if it can reasonably be assumed that it will reveal facts relevant to the criminal proceedings. Audio, video and audio video recording as well as interception and recording of the telecommunication operations do not have specific definitions according to national legislation, as stated above, tools are understood in rather broad concept and allow for using of various techniques and equipment.	• Code of Criminal Procedure 301/2005 Coll. • Article 113 (paragraph 1) • Article 114, 115
For what types of crime can the tool be used?	There are no restriction with respect to the specific types of the criminal activities where surveillance tools may be authorised. Tool may be performed in the criminal proceedings on an intentional criminal offence where thresholds indicated below are met.	• Code of Criminal Procedure 301/2005 Coll. • Article 113, 114, 115
Does national law allow this tool to be used in cross border cases?	Tool can be used for both national and cross border investigations; cross border use requires an international legal assistance request or cooperation within a Joint Investigation Team	• Code of Criminal Procedure 301/2005 Coll. • Article 531 - 540
What thresholds must be passed for the use of this tool?	1. There are no thresholds set in the legislation for the physical surveillance / observation 2. Audio, video or audio-video surveillance may be performed in criminal proceedings for an intentional criminal offense for which the law provides for a custodial sentence with a maximum penalty of more than three years, corruption or for another intentional criminal offense bound by an international treaty 3. Interception and recording of telecommunication operations may be performed in criminal proceedings on a crime (i.e. criminal offence with the minimum penalty of 5 years), corruption, a criminal offence of abuse of authority of a public official, a criminal offence of money laundering or another intentional criminal offence, the performance of which is bound by an international treaty	• Code of Criminal Procedure 301/2005 Coll. • Article 113, 114, 115
What types of stakeholder are involved in the implementation of this tool?	1. Judicial authorities - presiding judge approves the request of the respective LEA (Police Force or Criminal Office of the Financial Administration) and issues the warrant to execute physical surveillance / audio/video recording / interception and recording of telecommunication operations in cases when criminal proceedings have been already commenced. 2. Prosecutor approves the request of the respective LEA and issues the warrant to execute physical surveillance in cases prior the commencement of criminal proceedings or in the preparatory proceedings. Prosecutor also approves LEA requests and requests warrants in cases indicated below in point 3. 3. Judge for the preliminary proceedings approves the request of the respective LEA and the prosecutor and issues the warrant to execute audio/video recording / interception and recording of telecommunication operations in cases prior the commencement of criminal proceedings or in the preparatory proceedings. 4. Warrant issued by the judge for the preliminary proceedings in cases prior the commencement of criminal proceedings or in the preparatory proceedings is also required in cases where physical surveillance is requested in premises and areas that are not publicly accessible or physical surveillance using the technical means (e.g. GPS trackers) is requested. 5. LEA (Police Force and Criminal Office of the Financial Administration) - appointed LEA officer (investigator) issues a requests to perform physical surveillance / audio/video recording/interception and recording of telecommunication operations to be approved by respective judicial authority as indicated above (depending whether the criminal proceedings have been already commenced and what type of activity is requested. If the request is approved and the warrant issued, LEA officers perform the surveillance	• Code of Criminal Procedure 301/2005 Coll. • Article 113 (paragraph 2) • Article 114 (paragraph 2) • Article 115 (paragraph 2)
Which LEAs can use this tool?	Police Force and Criminal Office of the Financial Administration respectively to their competencies according to the Code of the Criminal Procedure.	• Act on Police Force 171/1993 Coll. • Article 36, 39 • Act on Financial Administration 35/2019 Coll. • Article 14, 16
What are the rules to be followed for the implementation of this tool?	Physical surveillance (observation) - The warrant for the surveillance under may be issued only on the basis of a written request from a police officer or the competent authority of the Police Force and, in proceedings before the court, upon the written request of the public prosecutor. The request must be justified by the	• Code of Criminal Procedure 301/2005 Coll. • Article 113 (paragraph 3 - 11) • Article 114 (paragraph 3 - 8) • Article 115 (paragraph 3 - 11)

Relevant items	Provisions	Sources used
	suspicion of the commission of a specific criminal activity and also by the data on the persons and items to be surveyed, provided such information is known. The warrant must specify the period during which the surveillance shall be performed and this must not be longer than six months. The person who issued the warrant for the surveillance may extend the surveillance period in writing, but by no more than another six months, and they may even do so repeatedly. If the surveillance lasts longer than twelve months, the warrant for the surveillance before the onset of the criminal prosecution and in the preliminary proceedings shall be issued by the judge for the preliminary proceedings. - A police officer or a competent department of the Police Force is obligated to systematically examine the duration of the reasons that led to the issue of surveillance warrant. If the reasons have expired, the surveillance must be terminated even before the lapse of the time specified in Subsection 5. This fact must be announced to the person who issued the warrant in writing and, in the preliminary proceedings, also to the public prosecutor without undue delay. Audio/video recording - A time period must be set at which the making of video, audio or video-audio recordings will be carried out; this period may not exceed six months. The person who issued the order to make video, audio or video-audio recordings may extend their duration in writing by a maximum of two months, even repeatedly. - Preparation of video, audio or video-audio records is performed by the Police Force. If, during the making of video, audio or video-audio recordings, it is found that the accused is communicating with his lawyer, the information thus obtained may not be used for the purposes of criminal proceedings and must be prescribed in a manner without destruction; this does not apply in the case of information which is held on a case in which the lawyer does not represent the accused as a lawyer. - A police officer or the competent department of the Police Force is obligated to systematically examine whether the reasons that led to the issue of the interception and recording of telecommunication operations warrant are still valid. If the reasons have expired, the interception and recording of telecommunication operations must be terminated, even before the lapse of the period for which the warrant was issued. The person who issued the warrant for the interception and recording of telecommunication operations and, in the preliminary proceedings also the public prosecutor, shall be notified. . Interception and Recording of the Telecommunication Operations - The warrant for the interception and recording of telecommunication operations must be issued in writing and must be justified by its merits, specifically for each user address or device. The warrant must include the determination of the user address or device and the person, if their identity is known, that the interception and recording of telecommunication operations concerns, and the period during which the interception and recording of telecommunication operations will be performed. - The interception and recording period may last up to six months. In the preliminary proceedings upon the petition of the public prosecutor, this period may be extended by the judge for the preliminary proceedings, but always by only two months although it can be done so repeatedly. - The interception and recording of telecommunication operations shall be performed by the competent department of the Police Force. Numerous other rules apply for the surveillance tools, especially for interception and recording of the telecommunication operations.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Tools can be used in the criminal procedure only with a warrant issued by a judge. Please refer to question regarding the authorisation needed for the use of this tool. Further safeguards regarding the Audio / video recording and Interception and recording of telecommunication operations are stipulated in the Act No. 166/2003 on Protection against Unlawful Use of Information and Technical Means (Wiretapping Protection Act). Act provides specification with respect to manipulation with intercepted communication and audio / video recordings and established a specialised Commission under the National Council of the Slovak Republic (i.e. Slovak Parliament) responsible for controlling the usage of the audio /video recording and interception and recording of telecommunication operations.	• Code of Criminal Procedure 301/2005 Coll. • Article 113 (paragraph 2) • Article 114 (paragraph 2) • Article 115 (paragraph 2) • • Act No. 166/2003 on Protection against Unlawful Use of Information and Technical Means (Wiretapping Protection Act). • Article 7 - 9
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Physical surveillance (observation): - The presiding judge, before the commencement of the criminal prosecution, or in the preliminary proceedings the public prosecutor, shall issue a warrant for surveillance in writing. - If it is necessary that the surveillance is performed in other premises or land that are not publicly accessible, or if the technical information resources are to be utilised during the surveillance and the surveillance is not associated with entry into a dwelling, the warrant for the surveillance shall be issued by the presiding judge, before the commencement of the criminal prosecution or in the preliminary proceedings, by the judge for preliminary proceedings upon the petition of the public prosecutor, if the facts important to the criminal proceedings cannot be obtained otherwise during the performance of surveillance; the warrant shall include the indication of other premises or land that are not publicly accessible where the surveillance is to	• Code of Criminal Procedure 301/2005 Coll. • Article 113 (paragraph 2) • Article 114 (paragraph 2) • Article 115 (paragraph 2)

Relevant items	Provisions	Sources used
	take place, and the type of technical information resources that are to be used. If the matter cannot be deferred, the judge for the preliminary proceedings of the court under which jurisdiction the surveillance is to be performed may issue the warrant instead of the competent judge for the preliminary proceedings. Upon entering non-residential premises or land that is not publicly accessible, no action other than that necessary to conduct the surveillance may be performed. Audio/video recording / Interception and recording of telecommunication operations: The warrant shall be issued by the presiding judge, before the onset of the criminal prosecution, or in the preliminary proceedings upon the petition of the public prosecutor, by the judge for the preliminary proceedings. If it is a matter that cannot be deferred and the audio/video recording / interception and recording of telecommunication operations is not associated with entry into a dwelling and a written warrant from the judge for the preliminary proceedings cannot be obtained in advance, the warrant may be issued before the commencement of the criminal prosecution or in the preliminary proceedings by the public prosecutor; the warrant must be confirmed by the judge for the preliminary proceedings no later than 24 hours from its issue, otherwise it shall expire and the information thus obtained cannot be used for the purposes of the criminal proceedings and must be destroyed in a prescribed manner without undue delay.	
What ongoing supervision is required for the use of this tool?	A police officer or the competent department of the Police Force is obligated to systematically examine whether the reasons that led to the issue of the interception and recording of telecommunication operations warrant are still valid. If the reasons have expired, the interception and recording of telecommunication operations must be terminated, even before the lapse of the period for which the warrant has been issued. The person who issued the warrant for the interception and recording of telecommunication operations and, in the preliminary hearing also the public prosecutor, shall be notified.	N/A
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Undercover / covert operations		
Relevant documents (legal and non-legal) that define the functioning of the tool	Code of Criminal Procedure 301/2005 Coll. Article 117 Act on Police Force 171/1993 Coll. Article 39a, 39b, 39c and 40 Act on Financial Administration 35/2019 Coll. Article 17	https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2005/301/20210101 https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1993/171/20200101 https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2019/35/20210301
How is the tool defined?	Criminal procedure code regulates under-cover investigation in section 117 on the use of agent. Use of agent is limited to crimes with the minimum penalty of 5 years, organised crime cases, corruption, extremist crimes, money laundering and abuse of authority of a public official. Undercover officers / covert operations may also be used outside the scope of the Criminal Procedure Code, for the purposes of criminal intelligence. Criminal intelligence means an activity by which information on criminal offenses and their perpetrators is obtained, collected and evaluated in a secret manner and conditions for the use of an agent are created.	- Code of Criminal Procedure 301/2005 Coll. - Article 117 (paragraph 1)
For what types of crime can the tool be used?	There are no restriction with respect to the specific types of the criminal activities where surveillance tools may be authorised. Tool may be performed in the criminal proceedings on an intentional criminal offence where thresholds indicated below are met.	- Code of Criminal Procedure 301/2005 Coll. - Article 117 (paragraph 1)
Does national law allow this tool to be used in cross border cases?	Tool can be used for both national and cross border investigations; cross border use requires an international legal assistance request or cooperation within a Joint Investigation Team	- Code of Criminal Procedure 301/2005 Coll. - Article 531 - 540
What thresholds must be passed for the use of this tool?	An agent may be used for the detection, investigation and conviction of offenders of crimes (criminal offence with the minimum penalty of 5 years), corruption, a criminal offence of abuse of authority of a public official, or a criminal offence of money laundering. Their use is permitted only if the detection, investigation and conviction of offenders of the listed criminal offences would otherwise be much more difficult, and the learned facts justify the suspicion that a criminal offence was committed or such criminal offence is to be committed.	- Code of Criminal Procedure 301/2005 Coll. - Article 117 (paragraph 1)
What types of stakeholder are involved in the implementation of this tool?	1. Judicial authorities - a warrant for the use of an agent shall be issued by the presiding judge, before the commencement of the criminal prosecution or in the preliminary hearing, by the judge for the preliminary hearing upon the petition of the public prosecutor, which must be justified by its merits. 2. LEA - Appointed police officers perform undercover investigations as agents according to warrant issued by respective judicial authority. Police force and Criminal Office of the Financial Administration may also use undercover officers and covert operations for the purposes of the criminal intelligence outside the scope of the Code of the Criminal Prosecution pursuant to Articles 39a, 39b, 39c and 40 of the Act on Police Force 171/1993 and Article 17 of the Act on Financial Administration 35/2019 respectively.	- Code of Criminal Procedure 301/2005 Coll. - Article 117 (paragraph 5)

Relevant items	Provisions	Sources used
Which LEAs can use this tool?	Police Force and Criminal Office of the Financial Administration	- Act on Police Force 171/1993 Coll. - Article 39a (paragraph 1) - Act on Financial Administration 35/2019 Coll. - Article 17
What are the rules to be followed for the implementation of this tool?	Basic rules are outlined in the Article 117 of the Criminal Procedure Code, e.g.: - The conduct of an agent must be in compliance with the purposes of this Act and must be proportionate to the illegality of the conduct, detection, investigation or conviction which they participate in. An agent must not proactively induce the commission of a criminal offence; this shall not apply if it is a criminal offence of bribery of a public official or a foreign public official, and the ascertained facts suggest that the offender would commit such a criminal offence even if the warrant to use an agent was not issued. - An agent acts under a temporary or permanent 'legend' or without a 'legend'. A 'legend' is a summary of covert data on the agent, particularly their identity, marital status, education and employment. - If it is necessary for the establishment or maintenance of a 'legend', it is possible to produce or use covert documents under the terms set out in a special Act. - The warrant for the use of an agent must be in writing and must specify the period, during which the agent shall be used. The period of the use of an agent cannot be longer than six months. This period may be extended by only two months by the presiding judge and, in the preliminary hearing upon the petition of the public prosecutor, the judge for the preliminary hearing, although they may do so repeatedly. - The documents relating to the use of an agent shall be entered into the file only if the public prosecutor proposes the performance of evidence in the indictment through the facts found by an agent. - An agent may enter a dwelling, when using their 'legend', with the consent of an authorised person. However, such consent may not be obtained on the basis of a sham right to enter. - The true identity of an agent acting under a 'legend' must remain secret even after the completion of their use. The true identity of an agent must be disclosed to the public prosecutor or the judge for the preliminary hearing who is competent to decide under Subsection 5 and 6, as well as to the presiding judge in the proceedings before the court upon their request. ..numerous other rules apply pursuant to provisions of Article 117 of the Criminal Procedure Code	- Code of Criminal Procedure 301/2005 Coll. - Article 117 (paragraph 2 - 14)
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Tool can be used in the criminal procedure only with a warrant issued by a judge. Please refer to question regarding the authorisation needed for the use of this tool.	- Code of Criminal Procedure 301/2005 Coll. - Article 117 (paragraph 5)
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	A warrant for the use of an agent shall be issued by the presiding judge, before the commencement of the criminal prosecution or in the preliminary hearing, by the judge for the preliminary hearing upon the petition of the public prosecutor, which must be justified by its merits. If it is a matter that cannot be deferred and the use of an agent is not associated with entry into the dwelling of another person, the public prosecutor may issue the warrant referred before the commencement of the criminal prosecution or even orally in the preliminary hearing on a provisional basis. However, such warrant must be confirmed in writing no later than 72 hours from its issue by the judge for the preliminary hearing, otherwise it shall expire. This shall not apply to the procedure under Subsection 2, when the warrant to use an agent may only be issued by the judge for the preliminary hearing.	- Code of Criminal Procedure 301/2005 Coll. - Article 117 (paragraph 5)
What ongoing supervision is required for the use of this tool?	National Legislation does not stipulate any specific ongoing supervision over this tool. Internal regulations and procedures are restricted for the personal of the respective units and are not publicly available	N/A.
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	Act on Police Force 171/1993 Coll. Article 41 Act on Financial Administration 35/2019 Coll. Article 19	https://www.slov-lex.sk/vyhľadavanie-pravnych-predpisov?text=171%2F1993 https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2019/35/20210301
Specific range of application of the tool	An individual who voluntarily, in a classified manner, provides information and services to the Police Force / Financial Administration in detecting criminal activity.	- Act on Police Force 171/1993 Coll. - Article 41 (paragraph 1) - Act on Financial Administration 35/2019 Coll.

Relevant items	Provisions	Sources used
How is the tool defined?	Voluntary providing of information and services to the Police Force / Financial Administration in detecting criminal activity in a classified manner.	- Article 19 (paragraph 1) - Act on Police Force 171/1993 Coll. - Article 41 (paragraph 1) - Act on Financial Administration 35/2019 Coll. - Article 19 (paragraph 1)
For what types of crime can the tool be used?	There are no restriction for Police Force with respect to the specific types of the criminal activities where informants may be used. Criminal Office of the Financial Administration may use informant in detection of criminal offences related to violation of tax regulation in the field of excise duties, violation of customs regulations and intentional criminal offenses committed by members of the financial administration in the performance of civil service or by employees of the financial directorate in the performance of work in the public interest.	- Act on Financial Administration 35/2019 Coll. - Article 19 (paragraph 1)
Does national law allow this tool to be used in cross border cases?	Tool can be used for both national and cross border investigations. No specific rules for the use in the international cooperation apply	
What thresholds must be passed for the use of this tool?	No thresholds are identified in national law provisions or legal norms.	
What types of stakeholder are involved in the implementation of this tool?	LEA - Police Force and Criminal Office of the Financial Administration	- Act on Police Force 171/1993 Coll. - Article 41 - Act on Financial Administration 35/2019 Coll. - Article 19
Which LEAs can use this tool?	Police Force Criminal Office of the Financial Administration	- Act on Police Force 171/1993 Coll. - Article 41 - Act on Financial Administration 35/2019 Coll. - Article 19
What are the rules to be followed for the implementation of this tool?	Detailed rules for the implementation of the tool are restricted for Personnel of the respective units and are not publicly available.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	No specific safeguard are stipulated in the national legislation	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	National Legislation does not stipulate any specific authorisation requirement for this tool. Internal regulations and procedures are restricted for the personal of the respective units and are not publicly available	
What ongoing supervision is required for the use of this tool?	National Legislation does not stipulate any specific form of ongoing supervision for this tool. Internal regulations and procedures are restricted for the personal of the respective units and are not publicly available	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Fictitious transfer		
Relevant documents (legal and non-legal) that define the functioning of the tool	Chapter 373 - Prevention of Money Laundering Act Chapter 37 - Customs Ordinance Act	
How is the tool defined?	<u>10.(1)</u> Where the Attorney General receives a request made by a judicial or prosecuting authority of any place outside Malta for the temporary seizure of all or any of the moneys or property, movable or immovable, of a person (hereinafter in this article referred to as "the accused") charged or accused in proceedings before the courts of that place of an offence consisting in an act or an omission which if committed in these Islands, or in corresponding circumstances, would constitute an offence under article 3, the Attorney General may apply to the Criminal Court for an order (hereinafter referred to as a "freezing order") having the same effect as an order as is referred to in article 22A(1) of the Dangerous Drugs Ordinance, and the provisions of the said article 22A shall, subject to the provisions of sub article (2) of this article, apply mutatis mutandis to that order.	Prevention of Money Laundering Act Chapter 373 Article 10
For what types of crime can the tool be used?	11.(1) A confiscation order made by a court outside Malta providing or purporting to provide for the confiscation or forfeiture of any property of or in the possession or under the control of any person described in the order shall be enforceable in Malta in accordance with the provisions of article 24D(2) to (11) of the Dangerous Drugs Ordinance.	

Relevant items	Provisions	Sources used
Does national law allow this tool to be used in cross-border cases?	(2) For the purposes of this article "confiscation order" includes any judgment, decision, declaration, or other order made by a court whether of criminal or civil jurisdiction providing or purporting to provide for the confiscation or forfeiture of property as is described in sub article (1).	Prevention of Money Laundering Act Chapter 373 Article 11
What thresholds must be passed for the use of this tool?		
What types of stakeholder are involved in the implementation of this tool?	Prevention of Money Laundering Act Chapter 373 Article 3	Prevention of Money Laundering Act Chapter 373 Article 3/31A
Which LEAs can use this tool?	3.(1) Any person committing any act of money laundering shall be guilty of an offence and shall, on conviction, be liable to a fine (multa) not exceeding two million and five hundred thousand euro (€2,500,000), or to imprisonment for a period not exceeding eighteen years, or to both such fine and imprisonment	Customs ordinance Chapter 37 (70C)
What are the rules to be followed for the implementation of this tool?		
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Customs ordinance Chapter 37 (70C)	
What authorisation is needed for the use of this tool?(e.g. senior police officer, prosecutor, judge, other)	70C. (1) For the purposes of investigation related to crimes of contraband, fraud, evasion of tax or duty, money laundering or financing of terrorism, in order to fulfil his obligations under customs laws, the Commissioner may, without prejudice to any obligation of professional secrecy imposed by an explicit provision of the law, demand and collect details of transactions that have taken place, are taking place or which still have to take place, both if involving the person or entity to which the demand is made and if the said transactions are between third parties, from any person or entity, and every said person or entity shall give to the Commissioner the requested details within the time frame established by him. The said obtained details may be used by the Commissioner as evidence in proceedings before any court. (2) When the Commissioner suspects that the details of transactions collected could amount to proof of the crimes of money laundering or financing of terrorism, the Commissioner shall pass on the said details to the Financial Intelligence Analysis Unit.31.(1) Where, following an analysis of a report received by the Unit under article 16(1)(a) and of any other information relevant to that report, the Unit is of the opinion that a reasonable suspicion of money laundering or funding of terrorism or a reasonable suspicion that property may have derived directly or indirectly from, or constitutes the proceeds of criminal activity subsists, an analytical report drawn up as is referred to under article16(1)(a) shall be transmitted to the Police for further investigation.(2) The provisions of sub-article (1) shall also apply mutatis mutandis to any knowledge or suspicion of money laundering or the underlying criminal activity, or funding of terrorism, which the Unit may have gathered or formed from information in its possession without having received any report as is referred to under sub-article (1).(3) Where the Unit transmits information to the Police in pursuance of the provisions of sub-articles (1) and (2) and a subject person over which another authority or agency has supervisory or regulatory functions is involved, the Unit shall inform the said authority or agency of actions taken.(4) Where the Unit transmits information to the Police in pursuance of sub-articles (1) and (2) it shall thereafter transmit to the Police any further relevant information in respect of the knowledge or suspicion communicated to the Police as aforesaid.	
What ongoing supervision is required for the use of this tool?	(5) The Police shall, upon request and in a timely manner, inform the Unit on the use made of information provided by the Unit under this article and on the outcome of any investigations carried out pursuant to the information provided.	
Is there any national case law relating to the use of this tool in cross-border crime cases?		
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	<u>Chapter 373 Article 31A.</u>	

Source: Author's own elaboration

Spain

Table 46 – Overview of national rules on investigative tools - Spain

Relevant items	Provisions	Sources used
Controlled Delivery		

Relevant items	Provisions	Sources used
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Procedure Law	https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036
How is the tool defined?	Controlled circulation or delivery shall be understood as the technique consisting in allowing illicit or suspected consignments of toxic drugs, psychotropic substances or other prohibited substances, the equipment, materials and substances referred to in the previous section, the substances for which they are has replaced the aforementioned, as well as the assets and proceeds from criminal activities typified in articles 301 to 304 and 368 to 373 of the Criminal Code, circulate through Spanish territory or leave or enter it without interference from the authority or its agents and under their supervision, in order to discover or identify the people involved in the commission of any crime related to said drugs, substances, equipment, materials, goods and profits, as well as providing assistance to foreign authorities for those same purposes	Art. 263 bis para 2
For what types of crime can the tool be used?	1) toxic drugs, narcotics or psychotropic substances as well as other prohibited substances. 2) protection of endangered plant and animal species, 3) currency counterfeiting, 4) counterfeiting of other means of payment, 5) illicit arms possession and trafficking.	1) Art. 263 bis (1), 2) articles 332 and 334; 3) art 386; 4) art. 399 bis and 5) art. 566, 568, and 569
Does national law allow this tool to be used in cross border cases?	a) Crimes of obtaining, illicit trafficking of human organs and transplantation of the same, provided for in article 156 bis of the Penal Code. b) Crime of kidnapping of persons provided for in articles 164 to 166 of the Penal Code. c) Crime of trafficking in human beings provided for in article 177 bis of the Penal Code. d) Crimes related to prostitution provided for in articles 187 to 189 of the Penal Code. e) Crimes against property and against the socio-economic order provided for in articles 237, 243, 244, 248 and 301 of the Penal Code. f) Crimes related to intellectual and industrial property provided for in articles 270 to 277 of the Penal Code. g) Crimes against the rights of workers provided for in articles 312 and 313 of the Penal Code h) Crimes against the rights of foreign citizens provided for in article 318 bis of the Penal Code. i) Crimes of trafficking in endangered species of flora or fauna provided for in articles 332 and 334 of the Penal Code. j) Crime of trafficking in nuclear and radioactive material provided for in article 345 of the Penal Code. k) Crimes against public health provided for in articles 368 to 373 of the Penal Code. l) Crimes of currency counterfeiting, provided for in article 386 of the Penal Code, and of forgery of credit or debit cards or traveller's checks, provided for in article 399 bis of the Penal Code. m) The crime of trafficking and depositing weapons, ammunition or explosives provided for in articles 566 to 568 of the Penal Code. n) Terrorism offenses set forth in articles 572 to 578 of the Penal Code. o) Crimes against the historical heritage provided for in article 2.1.e of Organic Law 12/1995, of December 12, on the repression of smuggling.	Art. 282 bis (4) para from 'a' to 'o'
What thresholds must be passed for the use of this tool?	YES. Controlled delivery will be made on a case-by-case basis and, at the international level, will be adapted to the provisions of international treaties	Art. 263 bis (3)
What types of stakeholder are involved in the implementation of this tool?	Anyone promoting, organising, coordinating or directing a criminal organisation shall be liable to a penalty of four to eight years' imprisonment if the organisation's aim or purpose is to commit serious crimes, and a penalty of three to six years' imprisonment in all other cases; and anyone taking active part in the organisation, belonging to it or cooperating with it financially or in any other way, shall be liable to penalties of two to five years' imprisonment if the purpose is to commit serious crimes, and one to three years' imprisonment in all other cases.	Section 570 bis (1) of criminal code
Which LEAs can use this tool?	1) Court System (Audiencia Nacional) - The Audiencia Nacional is a specialised judicial body, created with the main purpose of dealing with terrorist cases. The Criminal Chamber has also jurisdiction over important cases of economic and organised crime, as well as decisions about extradition and the execution of European arrest warrants. 2) Public Prosecution System (Fiscalía de la Audiencia Nacional) - The Fiscalía de la Audiencia Nacional represents the public prosecution service before the Audiencia Nacional in all cases but those where competence lies with one of the two specialised bodies listed below. This office is headed by the Fiscal General del Estado (Attorney General) 3) Public Prosecutor's Office against Drug Trafficking (Fiscalía Especializada 4) Central Unit for Economic and Financial Crime - Unidad Central de Delincuencia Económica y Financiera (UDEF) Antidroga) This office handles drug trafficking and money laundering cases under the jurisdiction of the Audiencia Nacional, including those with an organised crime component. It also coordinates the action of the rest of the Spanish public prosecution system in drug trafficking, money laundering related cases. 4) Public Prosecutor's Office against Corruption and Organised Crime (Fiscalía especializada contra la corrupción y la criminalidad organizada) This office handles 'especially relevant cases' indicated by the Attorney General for the following crimes: Tax fraud and contraband; Misconduct of executive or public official; Insider trading; Misuse of public funds; Illegal taxation; Trafficking; Bribery; Fraud;	Page 572-573 of AMOC study. Link - https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/20150312_1_amoc_report_020315_0_220_part_2_en.pdf

Relevant items	Provisions	Sources used
	Insolvency offences; Public procurement offences; Crimes regarding intellectual property and copyright infringement; Corporate offences; Money laundering and handling of criminally acquired goods (unless committed in relation with drug trafficking or terrorism). 5) Organised Crime Intelligence Unit – Centro de Inteligencia sobre el crimen organizado (CICO) This body is part of the Ministry of Interior and is placed under the direct supervision of the Secretario de Estado. The CICO centralizes the intelligence and coordinates investigating activities on organised crime. It publishes the 'Informe anual sobre la situación de la criminalidad organizada en España' (Annual Report on the Situation of Organised Crime in Spain) 6) Central Unit for Drugs and Organised Crime – Unidad Central de Drogas y Crimen - A special unit focusing on drug trafficking and organised crime in general. 7) This unit is specialised in cases pertaining to money laundering. The Activities of the UDEF have proven instrumental to the advance of organised crime investigations.	
What are the rules to be followed for the implementation of this tool?	LEAs (Public Prosecutor's Office on the authorisations and, if there is an open judicial procedure, to the Judge. of competent Instruction)	Art 263 bis (3) para 2
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	1) The administrative authorities in charge of public security and the prosecution of all crimes or some special crimes. 2) Employees or subordinates of the security police, whatever their denomination. 3) The Mayors, Deputy Mayors and mayors of the neighbourhood. 4) The Chiefs, Officers and individuals of the Civil Guard or of any other force destined to the persecution of criminals. 5) Los Serenos, Celadores and any other municipal urban or rural police officers. 6) The rangers of mountains, fields and crops, sworn or confirmed by the Administration. 7) Officials of the Special Corps of Prisons. 8) The judicial agents and subordinates of the Tribunals and Courts. 9) The personnel dependent on the Central Traffic Headquarters, in charge of the technical investigation of accidents.	Art. 283
What authorisation is needed for the use of this tool?	The undercover agent will be exempt from criminal responsibility for those actions that are a necessary consequence of the development of the investigation, provided that they keep due proportionality with the purpose of the investigation and do not constitute a provocation to the crime	Art 282 bis (5)
What ongoing supervision is required for the use of this tool?	It can be authorised by the investigative judge, the public prosecutor or certain high-ranked police officers then has to immediately report their decision to the public prosecutor or the investigating judge (in case there is a judicial investigation).	Art 263 bis (1)
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	The previous study's result matched with this findings.
Data available on the number of times this tool has been used for SOC cases	N/A	
Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	N/A	
How is the tool defined?	Spain relies on art. 41 of the Schengen agreement to allow for hot pursuit in organised crime cases.	The previous study's result matched with this findings.
For what types of crime can the tool be used?	N/A	The previous study's result matched with this findings.
Does national law allow this tool to be used in cross border cases?	N/A	The previous study's result matched with this findings.
What thresholds must be passed for the use of this tool?	N/A	The previous study's result matched with this findings.
What types of stakeholder are involved in the implementation of this tool?	N/A	The previous study's result matched with this findings.
Which LEAs can use this tool?	N/A	The previous study's result matched with this findings.
What are the rules to be followed for the implementation of this tool?	N/A	The previous study's result matched with this findings.
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	The previous study's result matched with this findings.
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	The previous study's result matched with this findings.

Relevant items	Provisions	Sources used
What ongoing supervision is required for the use of this tool?	N/A	The previous study's result matched with this findings.
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	The previous study's result matched with this findings.
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	The previous study's result matched with this findings.
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	Organic Law 19/1994, of December 23, on the protection of witnesses and experts in criminal cases.	https://www.boe.es/buscar/act.php?id=BOE-A-1994-28510
How is the tool defined?	In national law, the tool is not defined but it says - "The protection measures provided for in this Law are applicable to those who intervene in criminal proceedings as witnesses or experts«	Art 1 (1)
For what types of crime can the tool be used?	No mention of any crimes. It says 'serious danger'.	- Art. 1 (2) - Art. 3 (1)
Does national law allow this tool to be used in cross border cases?	N/A	The previous study's result matched with this findings.
What thresholds must be passed for the use of this tool?	N/A	The previous study's result matched with this findings.
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	Public Prosecutor or investigating judge	- Art. 3 (2) - Art 2 (a), (b), and ©
What are the rules to be followed for the implementation of this tool?	Once the circumstance foreseen in the previous article has been appreciated, the examining judge will agree with reasons, ex officio or at the request of a party, when he deems it necessary in view of the degree of risk or danger, the necessary measures to preserve the identity of the witnesses and experts, their domicile , profession and place of work, without prejudice to the action of contradiction that assists in the defense of the accused, being able to adopt the following decisions: a) That their name, surname, address, place of work and profession, or any other information that could be used to identify them, does not include in the proceedings carried out, a number or any other password may be used for this. b) That they appear for the practice of any diligence using any procedure that makes their normal visual identification impossible. c) That the domicile of the intervening judicial body be set as the domicile, for the purposes of subpoenas and notifications, which will send them confidentially to their addressee.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	no information found	The previous study's result matched with this findings.
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	LEAs	Art 2
What ongoing supervision is required for the use of this tool?	N/A	The previous study's result matched with this findings.
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Surveillance		
Relevant documents (legal and non-legal) that define the functioning of the tool	Organic Law 4/1997	https://www.boe.es/buscar/doc.php?id=BOE-A-1997-17574#:~:text=Ley%20Org%C3%A1nica%20de%2F1997%2C%20de,Ver%20texto%20consolidado&text=186%2C%20de%205%20de%20agosto,a%2023828%20(5%20p%C3%A1gs.%20)
Specific range of application of the tool	The national law does not have the Surveillance. It is specifically related to use of Camera by Police. Because of the violation of human rights, this law is not used much (my personal interpretation of the law 4/1997).	Art 1 (2)

Relevant items	Provisions	Sources used
How is the tool defined?	N/A	The previous study's result matched with this findings.
For what types of crime can the tool be used?	N/A	The previous study's result matched with this findings.
Does national law allow this tool to be used in cross border cases?	No. But Cross-border surveillance is authorised following article 40 of the Schengen agreement.	The previous study's result matched with this findings.
What thresholds must be passed for the use of this tool?	Does not have any laws in the national law no information found	The previous study's result matched with this findings.
What types of stakeholder are involved in the implementation of this tool?	LEAs	Art 1 (2)
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	Once the filming has been carried out in accordance with the requirements established in the Law, if the recording captures the commission of acts that could constitute criminal offenses, the Security Forces and Bodies will put the original tape or support of the images and sounds in their integrity to judicial disposition with the greatest immediacy possible and, in any case, within a maximum period of seventy-two hours from its recording. If the report cannot be drawn up within such period, the facts will be verbally reported to the judicial authority, or to the Public Prosecutor's Office, together with the delivery of the recording. Then The recordings will be destroyed within a maximum period of one month from their capture, unless they are related to serious or very serious criminal or administrative offenses in matters of public security, with an ongoing police investigation or with an open judicial or administrative procedure If the recording captures facts that could constitute administrative infractions related to citizen security, they will be sent to the competent body, also immediately, for the initiation of the appropriate sanctioning procedure.	- Art 7 (1), and (2) - Art 8 (1)
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Organic law 4/1997 establishes the regime of guarantees of the fundamental rights and public freedoms of citizens that must be respected inescapably in the successive phases of authorisation, recording and use of images and sounds obtained jointly by video cameras.	Art 1 para 2.
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Investigating judge or public prosecutor	Art. 3 (2) of Law no 19/94
What ongoing supervision is required for the use of this tool?	N/A	The previous study's result matched with this findings.
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Undercover / covert operations		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Procedure Law	https://www.boe.es/buscar/act.php?id=BOE-A-1882-6036
How is the tool defined?	Officials of the Judicial Police who have acted in an investigation with a false identity, may maintain said identity when they testify in the process that may arise from the events in which they have intervened and provided that this is the case It is agreed by means of a reasoned judicial resolution	Art 282 bis (2) para 2
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross border cases?	no information found in the national law but Spain has to follow Art 41 of Schengen Convention for cross-border cases.	The previous study's result matched with this findings.
What thresholds must be passed for the use of this tool?	no information found	The previous study's result matched with this findings.
What types of stakeholder are involved in the implementation of this tool?	LEAs and Police	Art 283 bis (6)
Which LEAs can use this tool?	Public Prosecutor or investigating judge	- Art 283 bis (1) - Art 283 (2)
What are the rules to be followed for the implementation of this tool?	by an investigating judge or a public prosecutor (in this latter case, she/he must immediately notify an investigating judge) - The decision must be grounded (according to Spanish law, all judicial decisions must be grounded) and must take into account the need of the covert investigation "in relation to the goals of the investigation".	

Relevant items	Provisions	Sources used
	- The decision must contain both the agent's real and "covert" name	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	1) No official of the Judicial Police may be forced to act as an undercover agent. 2) When the investigation actions may affect fundamental rights, the undercover agent must request from the competent judicial body the authorisations established	1) Art 282 bis (2) para 1. 2) Art 282 bis (3) para 2
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	With permission from public prosecutor, police can start surveillance area	Art 283 bis (6)
What ongoing supervision is required for the use of this tool?	N/A	The previous study's result matched with this findings.
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	This tool is not defined in the national law	The previous study's result matched with this findings.
Specific range of application of the tool	N/A	The previous study's result matched with this findings.
How is the tool defined?	N/A	The previous study's result matched with this findings.
For what types of crime can the tool be used?	N/A	The previous study's result matched with this findings.
Does national law allow this tool to be used in cross border cases?	N/A	The previous study's result matched with this findings.
What thresholds must be passed for the use of this tool?	N/A	The previous study's result matched with this findings.
What types of stakeholder are involved in the implementation of this tool?	N/A	The previous study's result matched with this findings.
Which LEAs can use this tool?	N/A	The previous study's result matched with this findings.
What are the rules to be followed for the implementation of this tool?	N/A	The previous study's result matched with this findings.
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	The previous study's result matched with this findings.
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	The previous study's result matched with this findings.
What ongoing supervision is required for the use of this tool?	N/A	The previous study's result matched with this findings.
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	The previous study's result matched with this findings.
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	The previous study's result matched with this findings.

Source: Author's own elaboration

Sweden

Table 47 – Overview of national rules on investigative tools - Sweden

Relevant items	Provisions	Sources used
Controlled Delivery		

Relevant items	Provisions	Sources used
Relevant documents (legal and non-legal) that define the functioning of the tool	The provisions on international legal assistance in criminal matters are mainly contained in the International Legal Assistance in Criminal Matters Act (2000:562). There are supplementary provisions on legal assistance in certain cases in the Act on Joint Investigation Teams for Criminal Investigations (2003:1174). The International Legal Assistance in Criminal Matters Act mainly consists of cooperation between prosecutors and courts. International police and customs collaboration is regulated by other laws. The Act does not cover extradition, surrender or the service of documents for which special legislation exists. Cooperation with international tribunals and the International Criminal Court is also regulated by other laws. The term Controlled Delivery is regulated in the term interim passivity. This is when the police postpone an intervention against a crime that the police normally would have intervened against. The purpose of the passivity is to secure evidence against the suspect. Interim passivity can be used when the police suspect that the person of interest is about to commit a new crime, as well as when the police do not have such suspicions. This method is mentioned as an admissible method in the preparatory work of the law on police activities	• https://www.government.se/government-of-sweden/ministry-of-justice/international-judicial-co-operation/legal-assistance-in-criminal-matters/ • The Swedish Code of Judicial Procedure: • https://www.regeringen.se/49bb67/contentassets/5503f73d320b4de5bb521dd7ee07500a/the-swedish-code-of-judicial-procedure • The Swedish criminal code: https://www.government.se/492a92/contentassets/7a2dcae0787e465e9a2431554b5eab03/the-swedish-criminal-code.pdf • https://lagrummet.se/English • Police Act (1984: 387) • SOU 1982: 63 Police Act report. • SOU 2003: 74 Increased efficiency and legal certainty in law enforcement. • Ds 2005: 21 Coercive measures to prevent or deter serious crime. • SOU 2010: 103 Special reconnaissance methods.
How is the tool defined?	Controlled delivery is the transport of objects from, into or through Sweden.	• Law (2003: 1174) on certain forms of international cooperation in criminal investigations.
For what types of crime can the tool be used?	Cross crime areas.	• Law (2003: 1174) on certain forms of international cooperation in criminal investigations.
Does national law allow this tool to be used in cross border cases?	Yes	• SFS nr: 1957:668 • The Swedish Code of Statutes (SFS) – the official and authentic version of acts, ordinances and government agency regulations. • https://svenskforfattningssamling.se/english.html • SFS nr: 1957:668
What thresholds must be passed for the use of this tool?	Since the use of the tool is not limited to certain types of crimes, there is no specific answer on the maximum imprisonment term for respective crimes. In general, the maximum term of imprisonment in Sweden is lifetime imprisonment.	• SFS nr: 1957:668
What types of stakeholder are involved in the implementation of this tool?	LEAs	• SFS nr: 1957:668
Which LEAs can use this tool?	The criminal police (the police section against international and serious organised crime) is the initiating and executing body. The use of the tool can also be initiated by foreign authorities. The prosecution is the authorising body.	• Law (2003: 1174) on certain forms of international cooperation in criminal investigations.
What are the rules to be followed for the implementation of this tool?	According to the recommendations stated by the Prosecuting Authority controlled delivery can be used to: a) obtain evidence of serious crime; b) be able to prevent another serious crime, c) be able to prosecute accomplices	• Law (2003: 1174) on certain forms of international cooperation in criminal investigations. • SOU 1982: 63 Police Act report. • SOU 2003: 74 Increased efficiency and legal certainty in law enforcement. • Ds 2005: 21 Coercive measures to prevent or deter serious crime. • SOU 2010: 103 Special reconnaissance methods.
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	A risk assessment must be made before an intervention is postponed. According to the recommendations, there may be reasons to intervene against crimes with a low penalty value, if there is a great risk of people being injured. In the same way, there may be reasons to postpone an intervention against a crime with a high penalty value, if the risk of injury to persons is low.	• The Public Prosecutor's Office report 1993: 3 - Memorandum regarding controlled deliveries of drugs, etc., p. 4
What authorisation is needed for the use of this tool?	Authorisation by the prosecution is needed before criminal police can use the tool.	• Law (2003: 1174) on certain forms of international cooperation in criminal investigations.
What ongoing supervision is required for the use of this tool?	There is no defined supervisory unit to observe the controlled delivery. However, it must always be designed in such a way that access to the suspects and the goods is possible at any time.	• Law (2003: 1174) on certain forms of international cooperation in criminal investigations. • SOU 1982: 63 Police Act report. • SOU 2003: 74 Increased efficiency and legal certainty in law enforcement. • Ds 2005: 21 Coercive measures to prevent or deter serious crime. • SOU 2010: 103 Special reconnaissance methods.
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	• SOU 1982: 63 Police Act report. • SOU 2003: 74 Increased efficiency and legal certainty in law enforcement. • Ds 2005: 21 Coercive measures to prevent or deter serious crime. • SOU 2010: 103 Special reconnaissance methods.
Data available on the number of times this tool has been used for SOC cases	N/A	
Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	There is no specific national law on hot pursuit in Sweden. Since the Convention implementing the Schengen Agreement (Schengen Convention) applies to Sweden, Art. 41 Schengen Convention is the basic relevant law.	• SFS Act (2017: 496) on international police cooperation • Schengen Convention: the Convention implementing the Schengen Agreement of 14 June 1985,

Relevant items	Provisions	Sources used
	Additionally, bilateral agreements exist for interstate police cooperation with all countries bordering Sweden (Denmark and Norway), all of them containing rules on hot pursuit. Those rules are mainly specifying Art. 41 Schengen Convention. All of the agreements are subject to cross-border police cooperation	- the agreement with Denmark: the agreement of 6 October 1999 between the Government of the Kingdom of Sweden and the Government of the Kingdom of Denmark on police cooperation in the Öresund region, - the Öresund connection: the fixed link across the Öresund as defined in Article 2 of the Agreement with Denmark, - Prüm Council Decision: Council Decision 2008/615 / JHA of 23 June 2008 on enhanced cross-border cooperation, in particular in the fight against terrorism and cross-border crime, - Atlas Council Decision: Council Decision 2008/617 / JHA of 23 June 2008 on enhanced cooperation in crisis situations between the specialised task forces of the Member States of the European Union, - The agreement with Norway: the agreement of 4 September 2018 between the Government of Sweden and the Government of Norway on mutual assistance between the police's special task forces in crisis situations, - Reference data: register data which do not reveal the identity of a person, either in the form of a numerical designation and a fingerprint or a numerical designation and a DNA profile from the non-coding part of the person's DNA, - the CBE Directive: Directive (EU) 2015/413 of the European Parliament and of the Council of 11 March 2015 on the facilitation of cross-border exchanges of information on road safety-related offenses, as originally worded, - VIS Council Decision: Council Decision 2008/633 / JHA of 23 June 2008 on access to the Visa Information System (VIS) for searches by the designated authorities of the Member States and for Europol for the purpose of preventing, detecting and investigating terrorist offenses and other serious offenses, and - Agreement with the United States of America: the Agreement of 16 December 2011 between the Government of the Kingdom of Sweden and the Government of the United States of America on enhanced cooperation in the prevention and fight against crime. Lag (2020: 80).
How is the tool defined?	Since the agreements with bordering countries mainly specify the ground rules set in the Schengen Convention, the Schengen Convention shall suffice as a reference here for consistency reasons. Schengen Convention: Officers of one of the Contracting Parties who are pursuing in their country an individual caught in the act of committing or of participating in one of the offences referred to in paragraph 4 shall be authorised to continue pursuit in the territory of another Contracting Party without the latter's prior authorisation where, given the particular urgency of the situation, it is not possible to notify the competent authorities of the other Contracting Party by one of the means provided for in Article 44 prior to entry into that territory or where these authorities are unable to reach the scene in time to take over the pursuit. The same shall apply where the person being pursued has escaped from provisional custody or while serving a sentence involving deprivation of liberty.	Art 41 para. 1 Schengen Convention
For what types of crime can the tool be used?	The following crime types are listed in Art 41 Schengen Convention: murder, manslaughter, rape, arson, forgery of money, aggravated burglary and robbery and receiving stolen goods, extortion, kidnapping and hostage taking, trafficking in human beings, illicit trafficking in narcotic drugs and psychotropic substances, breach of the laws on arms and explosives, wilful damage through the use of explosives, illicit transportation of toxic and hazardous waste, failure to stop and give particulars after an accident which has resulted in death or serious injury.	
Does national law allow this tool to be used in cross border cases?	The tool is specifically designed for cross-border cases.	
What thresholds must be passed for the use of this tool?	The tool can be used for various types of crimes. The sentences for these range up to life in prison.	
What types of stakeholder are involved in the implementation of this tool?	LEAs	
Which LEAs can use this tool?	Police directorate; Directorate General for the Public Security.	
What are the rules to be followed for the implementation of this tool?	The stakeholders involved vary slightly among the bilateral agreements. Obligations Section 1 Foreign officials shall, when exercising powers under this Act, comply with Swedish law and other statutes as well as instructions issued by the Police Authority or the Security Police. They must always be able to prove their competence and identity. Criminal law protection and liability Section 2 Foreign officials who exercise authority in Sweden in accordance with this Act shall be protected in accordance with Chapter 17. §§ 1, 2 and 4 of the Criminal Code in the same way as if it had been a question of Swedish exercise of authority.	

Relevant items	Provisions	Sources used
	Schengen Convention: Officers of one of the Contracting Parties who are pursuing in their country an individual caught in the act of committing or of participating in one of the offences referred to in paragraph 4 shall be authorised to continue pursuit in the territory of another Contracting Party without the latter's prior authorisation where, given the particular urgency of the situation, it is not possible to notify the competent authorities of the other Contracting Party by one of the means provided for in Article 44 prior to entry into that territory or where these authorities are unable to reach the scene in time to take over the pursuit. The same shall apply where the person being pursued has escaped from provisional custody or while serving a sentence involving deprivation of liberty.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	In order for the pursuit to continue, it is also required that the crossing of the border is reported to a competent Swedish authority as soon as possible and that the foreign authority requests assistance in the investigation without delay.	
What ongoing supervision is required for the use of this tool?	The police directorate of the territory where the border is to be crossed must be informed as soon as possible. Also, the Directorate General for the Public Security, situated in the interior ministry, must be informed.	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	In general, the person charged in court has the right to know the identity of witnesses. This is the case in Sweden in almost all cases (qualified protective identities are an exception). This makes witness protection limited. However there are three types of protected personal data, or protected identity as it is also called you can apply for: 1: confidentiality marking -A confidentiality mark is the lower degree of protected personal data. A confidentiality mark is an administrative measure that makes it more difficult for others to access your personal information in the population register. The privacy statement covers all your personal information. 2 protected population registration - When you have protected population registration, you may be registered in the old municipality even though you have moved from there, or in another municipality to which you have not had any connection. The old address information is deleted and the new address is not registered in the population register, and thus never spread to other authorities. An address to the Swedish Tax Agency is registered where you receive your mail. 3:: fictitious personal data You may receive fictitious personal data if you are the victim of a particularly serious crime and are threatened with your life, health or liberty. This means that you receive new identity information, such as a new name and a new social security number. You apply for fictitious personal information with the Police. In ordinance (2006: 519) on special personal safety work etc. states which criteria must be met in order for special personal safety work to be carried out. In the first instance, special personal security work is carried out for witnesses, informants, employees in the judiciary or relatives of these. The police authority is responsible for the special personal security work. The Swedish Prison and Probation Service is, however, responsible for special personal security work regarding those who are serving prison sentences. The Swedish Security Police also are allowed to use this tool.	• Ordinance (2014: 1103) with instructions for the Security Police • Ordinance (2006: 519) on special personal safety undertaking, etc. • Swedish Tax Agency (for protected identity) • https://polisen.se/siteassets/forfattningssamling/fap-nummer/fap480_1_pmfs2016_11.pdf • http://www.regeringen.se/sb/d/108/a/392 • http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Polislag-1984387_sfs-1984-387/ • http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Forordning-2006519-om-sarsk_sfs-2006-519/

Relevant items	Provisions	Sources used
How is the tool defined?	A primary precondition for a person being accepted into the programme is that there is a manifest risk of criminality that is directed against his or her or a closely related person's life, health, liberty or freedom. 1. suspects, defendants, plaintiffs, witnesses and others who participate or have participated in a preliminary investigation or trial involving serious or organised crime (witnesses); 2. persons who continuously provide or have provided information to the Police Authority or the Security Police in matters relating to serious or organised crime; 3. employees of the judiciary, or 4. relatives of persons listed in 1-3.	• Ordinance (2014: 1103) with instructions for the Security Police • Ordinance (2006: 519) on special personal safety undertaking, etc.
For what types of crime can the tool be used?	none of the relevant tools relates to certain crime types as a condition for the use of the tool.	
Does national law allow this tool to be used in cross border cases?	The Chief of the National Police or the head of the National Operations Department at the Police Authority may, on behalf of the Police Authority, enter into an agreement with a foreign law enforcement authority on co-operation regarding special personal security work.	
What thresholds must be passed for the use of this tool?	none of the relevant tools relates to certain crime types as a condition for the use of the tool.	
What types of stakeholder are involved in the implementation of this tool?	LEAs, Judicial Authority.	
Which LEAs can use this tool?	The police authority is responsible for the special personal security work. The Swedish Prison and Probation Service is, however, responsible for special personal security work regarding those who are serving prison sentences. The Swedish Security Police also are allowed to use this tool.	• Ordinance (2014: 1103) with instructions for the Security Police • Ordinance (2006: 519) on special personal safety undertaking, etc.
What are the rules to be followed for the implementation of this tool?	A primary precondition for a person being accepted into the programme is that there is a manifested risk that is directed against his or her or a closely related person's life, health, liberty or freedom. Personal security programs (witness protection) should only be applied in cases where there are no other sufficient measures .	• SOU 2004:1, p.125 • See Appendix A for the Personal Security Inquiry's (SOU 2004: 1) constitutional proposal for personal safety law. • SOU 2004:1, p.16, p.131. • SOU 2004:1, p.129. • SOU 2004:1, p.144. • SOU 2004:1, p.141. • SOU 2004:1, p.133. • SOU 2004:1, p.128. • SOU 2004:1, p.132.
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Surveillance		
Relevant documents (legal and non-legal) that define the functioning of the tool	For cross border: Law on International Legal Assistance in Criminal Matters. Assistance for covert interception, including bugging, may be provided to other states. Swedish authorities can also carry out the measures on behalf of foreign states. Such measures shall be tried in accordance with the general provisions on coercive measures in accordance with Swedish law.	• Law (2012:278) on the collection of data on electronic communications in law enforcement authorities' intelligence activities • Secret coercive measures • [K27] 18 § and 19 §
Specific range of application of the tool	-tracking surveillance: locating a technical device -visual surveillance -acoustic surveillance -intercepting mails -surveillance of messages	• Law (2012:278) on the collection of data on electronic communications in law enforcement authorities' intelligence activities • Secret coercive measures • [K27] 18 § and 19 § - The Swedish Code of Judicial Procedure
How is the tool defined?	detention of mail (post control), secret interception of electronic communications	• Law (2012:278) on the collection of data on electronic communications in law enforcement authorities' intelligence activities

Relevant items	Provisions	Sources used
	covert surveillance of electronic communications secret camera surveillance secret room interception secret data reading	• Secret coercive measures • [K27] 18 § and 19 § - The Swedish Code of Judicial Procedure
For what types of crime can the tool be used?	Cross crime areas. Section 130 para. 1 CCP states: Surveillance is permissible if it appears necessary to solve a criminal offence or to find out the whereabouts of the suspect.	• Law (2012:278) on the collection of data on electronic communications in law enforcement authorities' intelligence activities • Secret coercive measures • [K27] 18 § and 19 § - The Swedish Code of Judicial Procedure
Does national law allow this tool to be used in cross border cases?	For cross border: Law on International Legal Assistance in Criminal Matters. Assistance for covert interception, including bugging, may be provided to other states. Swedish authorities can also carry out the measures on behalf of foreign states. Such measures shall be tried in accordance with the general provisions on coercive measures in accordance with Swedish law.	• Law (2012:278) on the collection of data on electronic communications in law enforcement authorities' intelligence activities • Secret coercive measures • [K27] 18 § and 19 § - The Swedish Code of Judicial Procedure
What thresholds must be passed for the use of this tool?	Covert interception is considered to be more intrusive and intrusive than covert surveillance, which means that higher requirements are set in the 27:18 Code of Judicial Procedure, e.g. that it must be a question of a crime for which no lesser punishment than imprisonment for two years is prescribed (cf. six months in the 27:19 Code of Judicial Procedure). A permit for covert interception also entails a right to covert surveillance, but not the other way around.	• Law (2012:278) on the collection of data on electronic communications in law enforcement authorities' intelligence activities • Secret coercive measures • [K27] 18 § and 19 § - The Swedish Code of Judicial Procedure
What types of stakeholder are involved in the implementation of this tool?	LEAs, Judicial Authority.	• Law (2012:278) on the collection of data on electronic communications in law enforcement authorities' intelligence activities • Secret coercive measures • [K27] 18 § and 19 § - The Swedish Code of Judicial Procedure
Which LEAs can use this tool?	Criminal Police, Public Prosecution, Security Police	• Law (2012:278) on the collection of data on electronic communications in law enforcement authorities' intelligence activities • Secret coercive measures • [K27] 18 § and 19 § - The Swedish Code of Judicial Procedure
What are the rules to be followed for the implementation of this tool?	For all use of coercive measures, three general principles are considered to apply; the principle of purpose, the principle of necessity and the principle of proportionality. In addition to the fact that the suspected crimes must, as a general rule, result in imprisonment for a certain period of time, other requirements are also set for the court to be able to decide that a secret coercive measure may be used. In the vast majority of cases, it is required that the person who is subjected to a secret coercive measure is reasonably suspected of the crime. A decision on a secret coercive measure is in principle never valid for more than one month from the date of the decision. After that, a new decision must be made.	• Law (2012:278) on the collection of data on electronic communications in law enforcement authorities' intelligence activities • Secret coercive measures • [K27] 18 § and 19 § - The Swedish Code of Judicial Procedure
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Secret data reading according to the first paragraph may only refer to a readable information system that has been used in a crime or in connection with a crime scene at the time of the crime or which for some other reason is of particular importance to the investigation. Section 11 A permit for secret data reading may not refer to a readable information system that is permanently used or is specifically intended to be used: 1. in activities where the duty of confidentiality applies according to ch. Section 3 of the Freedom of the Press Ordinance or Chapter 2 Section 3 of the Freedom of Expression Act, 2. in activities conducted by lawyers, doctors, dentists, midwives, nurses, psychologists, psychotherapists or family counsellors in accordance with the Social Services Act (2001: 453), or 3. by priests in denominations or by those who have a similar position in such denominations, in activities for confession or individual pastoral care.	• Law (2012:278) on the collection of data on electronic communications in law enforcement authorities' intelligence activities • Secret coercive measures • [K27] 18 § and 19 § - The Swedish Code of Judicial Procedure
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	According to the Code of Judicial Procedure, covert coercive measures may only be used for the purposes specified in law (the principle of purpose) if less intrusive measures have proved insufficient (the principle of need) and in addition the use may only have a scope and duration that is in reasonable proportion (principle of proportionality).	• Law (2012:278) on the collection of data on electronic communications in law enforcement authorities' intelligence activities • Secret coercive measures • [K27] 18 § and 19 § - The Swedish Code of Judicial Procedure
What ongoing supervision is required for the use of this tool?	Besides the authorisation chain, there is no indication for continuous supervision in case the tool comes to use.	
Is there any national case law relating to the use of this tool in cross-border crime cases?		
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	Covert eavesdropping on electronic communications has included 1,378 persons in 2017, which means an increase compared to 2016 when 1,253 people were intercepted.	• Government letter 2018/19: 19 • Account of the use of secret coercive measures in 2017 • https://data.riksdagen.se/fil/430817C6-955B-44F7-B7DE-BA4159713515
Undercover / covert operations		

Relevant items	Provisions	Sources used
Relevant documents (legal and non-legal) that define the functioning of the tool		- Police Act (1984: 387) - Act (2020: 62) on secret data reading
How is the tool defined?	The term unconventional reconnaissance methods is a collective name for various types of reconnaissance methods such as provocation, infiltration, agency activities, disinformation and secret interception.	Police Act (1984: 387)
For what types of crime can the tool be used?	Cross crime areas. Covert investigations are permitted if they appear necessary to solve a criminal offence. Fictitious purchases are permitted for the purpose of solving a crime or for securing objects or assets. But The police may never, according to these principles: commit a crime or a criminal act in order to investigate or expose a crime, provoke or persuade someone to start a criminal activity or fail to take prescribed action against a crime or against a person suspected of a crime.	- Police Act (1984: 387) - Act (2020: 62) on secret data reading - Secret coercive measures [K27] 18 § and 19 § - The Swedish Code of Judicial Procedure
Does national law allow this tool to be used in cross border cases?	Act (2000: 562) contains among others: 6. covert interception of electronic communications and covert surveillance of electronic communications; 7. secret camera surveillance, 8. secret room interception, 9. secret data reading, 10. technical assistance with secret interception of electronic communications, secret surveillance of electronic communications and secret data reading in accordance with section 2, first paragraph 1 and 2 of the Act (2020: 62) on secret data reading, 11. permission for cross-border secret interception of electronic communications, secret surveillance of electronic communications and secret data reading in accordance with section 2, first paragraph 1 and 2 of the Secret Data Reading Act;	Act (2000: 562) on international legal assistance in criminal cases
What thresholds must be passed for the use of this tool?	Covert investigations are permitted if they appear necessary to solve a criminal offence. Fictitious purchases are permitted for the purpose of solving a crime or for securing objects or assets. Therefore, no specific terms of imprisonment are tied to the tools and imprisonment times theoretically can range up to life imprisonment.	- Police Act (1984: 387) - Act (2020: 62) on secret data reading - Secret coercive measures [K27] 18 § and 19 § - The Swedish Code of Judicial Procedure
What types of stakeholder are involved in the implementation of this tool?	LEAs	
Which LEAs can use this tool?	Criminal Police, Public Prosecution.	
What are the rules to be followed for the implementation of this tool?	Covert investigations that are not carried out systematically and over a longer period of time can be carried out by the police without further authorisation. Other investigations must be ordered by the public prosecution. Fictitious purchases must be ordered by the public prosecution, except if the purchase serves to secure drugs or counterfeit money.	- The Police Act (1984: 387) - The Police Ordinance (2014: 1104) - The ordinance (2014: 1103) with instructions for the Security Police
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	Besides the authorisation chain, there is no indication for continuous supervision in case the tool comes to use.	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	The informants activities form part of the intelligence activities' process for which the national operational department has procedural responsibility	The Police Authority's guidelines for informants activities (PM 2017: 54)
Specific range of application of the tool	Police use of informants and infiltrators constitute so-called unconventional reconnaissance methods. Such methods are mainly used in serious or organised crime such as drug offenses.	- Police Act (1984: 387) - SFS Act (2006: 939) on qualified protection identities § 3. - SOU 2010: 103 s 20, 112.

Relevant items	Provisions	Sources used
	The National Police Board's guidelines have been replaced by the Police Authority's guidelines for informant activities, where regulations on how the use of informants as a police officer working method is to be conducted, organised and administered can be found. Sweden otherwise lacks legal provisions and guidelines that are specifically aimed at infiltration. This working method must relate to the Police Act and the general public the powers provided for there.	
How is the tool defined?	An informant is a private person who in one way or another has contact with a criminal network and passively provides reliable information about this network to the police. The informant is not subordinate to the police but is completely independent of the police activities. The informant, on the other hand, is aware that the information provided will be part of the police's law enforcement work.	The Police Authority's guidelines for informants activities (PM 2017: 54)
For what types of crime can the tool be used?	Cross crime areas. No special type of crime is needed.	The Police Authority's guidelines for informants activities (PM 2017: 54)
Does national law allow this tool to be used in cross border cases?	N/A - meaning no special law regulates use of informants for cross border activities.	- Police Act (1984: 387) - SFS Act (2017: 496) on international police cooperation - Schengen Convention: the Convention implementing the Schengen Agreement of 14 June 1985, - the agreement with Denmark: the agreement of 6 October 1999 between the Government of the Kingdom of Sweden and the Government of the Kingdom of Denmark on police cooperation in the Öresund region, - the Öresund connection: the fixed link across the Öresund as defined in Article 2 of the Agreement with Denmark, - Prüm Council Decision: Council Decision 2008/615 / JHA of 23 June 2008 on enhanced cross-border cooperation, in particular in the fight against terrorism and cross-border crime, - Atlas Council Decision: Council Decision 2008/617 / JHA of 23 June 2008 on enhanced cooperation in crisis situations between the specialised task forces of the Member States of the European Union, - The agreement with Norway: the agreement of 4 September 2018 between the Government of Sweden and the Government of Norway on mutual assistance between the police's special task forces in crisis situations, - reference data: register data which do not reveal the identity of a person, either in the form of a numerical designation and a fingerprint or a numerical designation and a DNA profile from the non-coding part of the person's DNA, - the CBE Directive: Directive (EU) 2015/413 of the European Parliament and of the Council of 11 March 2015 on the facilitation of cross-border exchanges of information on road safety-related offenses, as originally worded, - VIS Council Decision: Council Decision 2008/633 / JHA of 23 June 2008 on access to the Visa Information System (VIS) for searches by the designated authorities of the Member States and for Europol for the purpose of preventing, detecting and investigating terrorist offenses and other serious offenses, and - Agreement with the United States of America: the Agreement of 16 December 2011 between the Government of the Kingdom of Sweden and the Government of the United States of America on enhanced cooperation in the prevention and fight against crime. Lag (2020: 80).
What thresholds must be passed for the use of this tool?	The use of informants and infiltrators is so-called unconventional reconnaissance methods. Such methods are mainly used in serious or organised crime such as drug offenses. Therefore, no specific terms of imprisonment are tied to the tools and imprisonment times theoretically can range up to life imprisonment.	- Police Act (1984: 387) - SFS Act (2006: 939) on qualified protection identities § 3. - SOU 2010: 103 s 20, 112. - The Police Authority's guidelines for informants activities (PM 2017: 54)
What types of stakeholder are involved in the implementation of this tool?	LEAs	- Police Act (1984: 387) - SFS Act (2006: 939) on qualified protection identities § 3. - SOU 2010: 103 s 20, 112.
Which LEAs can use this tool?	Criminal Police, Public Prosecution.	- Police Act (1984: 387) - SFS Act (2006: 939) on qualified protection identities § 3. - SOU 2010: 103 s 20, 112.
What are the rules to be followed for the implementation of this tool?	Covert investigations that are not carried out systematically and over a longer period of time can be carried out by the police without further authorisation. Other investigations must be ordered by the public prosecution.	- Police Act (1984: 387) - SFS Act (2006: 939) on qualified protection identities § 3. - SOU 2010: 103 s 20, 112.
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	According to Section 8.1 of the Police Authority's guidelines stipulates that an adult who has undergone a risk analysis can become an informant. The risk analysis is based on an investigation of the person's age, health and social situation. The person must be suitable for the task at all levels and be well	

Relevant items	Provisions	Sources used
	understood with the task. The informant must have access to information that can benefit police law enforcement. The informant holds his assignment as long as he agrees to it.	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	The police officer who has direct contact with the informant is called a handler. The task as a handler is limited to six years and may, if there are special reasons, be extended at two-year intervals.	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	Swedish courts have ruled in close to 500 applications for secret data reading, according to figures from the Security and Integrity Protection Board, the number approved is classified.	https://sverigesradio.se/artikel/polisen-anvander-spionprogram-mer-an-vantat

Source: Author's own elaboration

Switzerland

Table 48 – Overview of national rules on investigative tools - Switzerland

Relevant items	Provisions	Sources used
Controlled Delivery		
Relevant documents (legal and non-legal) that define the functioning of the tool	Federal Act on International Mutual Assistance in Criminal Matters (Rechtshilfegesetz, IRSG) European Convention on Extradition (Europäisches Auslieferungsübereinkommen) Bilateral or multilateral agreements (if applicable)	- Federal Act on International Mutual Assistance in Criminal Matters (Rechtshilfegesetz, IRSG) https://www.fedlex.admin.ch/eli/cc/1982/846_846_846/en - Europäisches Auslieferungsübereinkommen https://www.fedlex.admin.ch/eli/cc/1967/814_854_850/de
How is the tool defined?	Investigative tool permitting transportations of illegal or suspect consignments to enter, cross or exit the Swiss territory.	
For what types of crime can the tool be used?	It can be more or less extended according to the legal provisions / bilateral agreements (for instance drugs, firearms, explosives, counterfeit money, stolen or concealed goods, laundered cash)	
Does national law allow this tool to be used in cross border cases?	Yes	
What thresholds must be passed for the use of this tool?	A controlled delivery is used in case of the investigation would be impossible or significantly more difficult without such a measure	
What types of stakeholder are involved in the implementation of this tool?	Competent justice authority + competent law enforcement agency	
Which LEAs can use this tool?	Police, Customs	
What are the rules to be followed for the implementation of this tool?	The consignment must be permanently be surveilled Other rules may be applicable according to the specific legal provisions / bilateral agreements, for instance: Officers are prohibited from entering property that is not accessible to the public. They may enter work, business or commercial premises accessible to the public during their opening hours (<i>bilateral agreement Switzerland-Germany</i>).	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Swiss Criminal Procedure Code	
What authorisation is needed for the use of this tool?	Justice authorisation is mandatory Date: 5 December 2000 Summary: The complainant disputed the local jurisdiction of the Swiss authorities to prosecute and assess the accusation of money laundering, since the border control took place on German territory. According to the Framework Agreement, the Swiss authorities are competent to prosecute and Swiss law is applicable if the criminal conduct is connected with the border crossing. In the case of money laundering through international money transports, prosecution can also take place in the transit state Date: 29 April 2002	- Official Collection of the Decisions of the Federal Tribunal" ("Amtliche Sammlung der Entscheidungen des schweizerischen Bundesgerichts (BGE) 127 IV 20 https://www.bger.ch/ext/eurospider/live/de/php/clir/http/index.php?lang=de&type=highlight_simple_query&page=1&from_date=&to_date=&from_year=2000&to_year=2021&sort=relevance&subcollection_c6=on&insertion_date=&from_date_push=&top_subcollection_clir=any&query_words=einfuhr+drogen&part=all&de_fr=&de_it=&fr_de=&fr_it=&it_de=&it_fr=&orig=&translation=&rank=6&highlight_docid=atf%3A%2F%2F127-IV-20%3Ade&number_of_ranks=63&aazclir=clir - Official Collection of the Decisions of the Federal Tribunal" ("Amtliche Sammlung der Entscheidungen des schweizerischen Bundesgerichts (BGE)

Relevant items	Provisions	Sources used
	Summary: The President of the Criminal Court of Leventina, located in Bellinzona, found B. guilty in particular of trafficking in human beings, Money laundering by sending abroad at least CHF 10,000 of criminal origin; and Infringement and violation of the Federal Law on the Residence and Settlement of Foreigners, because he facilitated the illegal entry and residence and because he employed without authorisation an undetermined number of foreign women who are not authorised to work in Switzerland.	128 IV 117 https://www.bger.ch/ext/eurospider/live/de/php/clir/http/index.php?lang=de&type=highlight_simple_query&page=3&from_date=&to_date=&from_year=2000&to_year=2021&sort=relevance&subcollection_c6=on&insertion_date=&from_date_push=&top_subcollection_clir=any&query_words=einfuhr+ODER+ausfuhr+UND+illegal&part=all&de_fr=&de_it=&fr_de=&fr_it=&it_de=&it_fr=&orig=&translation=&rank=30&highlight_docid=atf%3A%2F%2F128-IV-117%3Ade&number_of_ranks=88&aazclir=clir
What ongoing supervision is required for the use of this tool?	See above	
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Data available on the number of times this tool has been used for SOC cases	Federal Act on International Mutual Assistance in Criminal Matters (Rechtshilfegesetz, IRSG) European Convention on Extradition (Europäisches Auslieferungsübereinkommen)	- Federal Act on International Mutual Assistance in Criminal Matters (Rechtshilfegesetz, IRSG) https://www.fedlex.admin.ch/eli/cc/1982/846_846_846/en - Europäisches Auslieferungsübereinkommen https://www.fedlex.admin.ch/eli/cc/1967/814_854_850/de
Hot pursuit		
Relevant documents (legal and non-legal) that define the functioning of the tool	Switzerland is part of the Schengen Convention as agreed in the Schengen Association Agreement and will therefore apply the relevant provisions of these instruments. Bilateral and multilateral agreements exist for interstate police cooperation with all countries bordering Switzerland. All of the agreements are subject to cross-border police cooperation. The agreement partners in specific are: -Germany -Italy -Austria -Liechtenstein -France Further agreements on police cooperation in combating crime include agreements with - Albania - Bosnia-Herzegovina - Hungary - Kosovo - Latvia - Macedonia - Montenegro - Serbia - Slovenia - and others.	- Schengen Association Agreement (SAA): https://www.fedlex.admin.ch/eli/cc/2008/113/de - Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22008A0227(03)&from=EN - Agreement with the European Police Office (Europol) https://www.fedlex.admin.ch/eli/cc/2006/181/de - Agreement with Austria: https://www.fedlex.admin.ch/eli/cc/2017/442/de - Agreement with Germany: https://www.fedlex.admin.ch/eli/cc/2003/184/de - Agreement with Italy: https://www.fedlex.admin.ch/eli/cc/2016/609/de - Agreement with France: https://www.fedlex.admin.ch/eli/cc/2009/460/de - Agreement with Liechtenstein: https://www.fedlex.admin.ch/eli/cc/2017/442/de - Others: https://www.fedlex.admin.ch/de/cc/international-law/0.36
How is the tool defined?	N/A	
For what types of crime can the tool be used?	In cross border cases, it depends on the legal provisions. Categories of crimes are specified (CH-FR) or crime must be an extraditable offence (CH-DE)	
Does national law allow this tool to be used in cross border cases?	Yes	
What thresholds must be passed for the use of this tool?	In general terms : a cross border hot pursuit can be engaged against a person who has be caught in the act of committing / participating in the commission of an extraditable crime	
What types of stakeholder are involved in the implementation of this tool?	Competent law enforcement agency and according to the situation competent justice authority	
Which LEAs can use this tool?	Police, Customs	
What are the rules to be followed for the implementation of this tool?	Requested bordering country must be immediately informed in case of an ongoing hot pursuit, if possible before crossing the border Hot pursuit must be interrupted if requested by the competent authority of the contracting state in whose territory they operate Other rules may be applicable according to the specific legal provisions / bilateral or multilateral agreements, for instance the acting officers shall comply with the legal provisions of the contracting state in whose territory they operate, etc.	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	Swiss Criminal Procedure Code	

Relevant items	Provisions	Sources used
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Date: 13 December 2016 Summary: The public prosecutor's office in CH conducted a criminal investigation against the German citizen X. When the latter moved his residence to Germany, the public prosecutor's office in CH requested the Chief Public Prosecutor in Cologne to take over the prosecution. After the prosecution was assigned to the German prosecution authorities, the proceedings pending in CH were suspended and the person was charged with the Swiss costs of the proceedings. However, it was found that after the prosecution has been transferred to a foreign country, the Swiss criminal authorities may no longer decide on a possible imposition of costs themselves and are bound by the decision on costs of the foreign authority. In particular, it is inadmissible to impose the Swiss costs of proceedings on the person prosecuted if the proceedings abroad have been discontinued due to the statute of limitations.	- Official Collection of the Decisions of the Federal Tribunal" ("Amtliche Sammlung der Entscheidungen des schweizerischen Bundesgerichts (BGE) 143 IV 91 https://www.bger.ch/ext/eurospider/live/de/php/clir/http/index.php?lang=de&type=highlight_simple_query&page=1&from_date=&to_date=&from_year=2000&to_year=2021&sort=relevance&subcollection_c6=on&insertion_date=&from_date_push=&top_subcollection_clir=any&query_words= strafverfolgung+im+ausland&part=all&de_fr=&de_it=&fr_de=&fr_it=&it_de=&it_fr=&orig=&translation=&rank=1&highlight_doid=atf%3A%2F%2F143-IV-91%3Ade&number_of_ranks=17&aclir=clir
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	Switzerland is part of the Schengen Convention as agreed in the Schengen Association Agreement and will therefore apply the relevant provisions of these instruments. Bilateral and multilateral agreements exist for interstate police cooperation with all countries bordering Switzerland. All of the agreements are subject to cross-border police cooperation. The agreement partners in specific are: -Germany -Italy -Austria -Liechtenstein -France Further agreements on police cooperation in combating crime include agreements with - Albania - Bosnia-Herzegovina - Hungary - Kosovo - Lettland - Macedonia - Montenegro - Serbia - Slovenia and others.	- Schengen Association Agreement (SAA): https://www.fedlex.admin.ch/eli/cc/2008/113/de - Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22008A0227(03)&from=EN - Agreement with the European Police Office (Europol) https://www.fedlex.admin.ch/eli/cc/2006/181/de - Agreement with Austria: https://www.fedlex.admin.ch/eli/cc/2017/442/de - Agreement with Germany: https://www.fedlex.admin.ch/eli/cc/2003/184/de - Agreement with Italy: https://www.fedlex.admin.ch/eli/cc/2016/609/de - Agreement with France: https://www.fedlex.admin.ch/eli/cc/2009/460/de - Agreement with Liechtenstein: https://www.fedlex.admin.ch/eli/cc/2017/442/de - Others: https://www.fedlex.admin.ch/de/cc/international-law/0.36
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	
Witness protection		
Relevant documents (legal and non-legal) that define the functioning of the tool	Federal law on the extrajudicial protection of witnesses (Bundesgesetz über den ausserprozessualen Zeugenschutz, ZeugSG)	SR 312.2 - Bundesgesetz vom 23. Dezember 2011 über den ausserprozessualen Zeugenschutz (ZeugSG) (admin.ch)
How is the tool defined?	The act regulates the implementation of witness protection programs for persons who are at risk due to their participation in criminal proceedings; and the establishment of the Federal Witness Protection Office and its duties.	Chapter 1 Art 1 ZeugSG
For what types of crime can the tool be used?	cross crime areas	- ZeugSG - Chapter 4 Art 28 ZeugSG - Chapter 1 Art 2 ZeugSG
Does national law allow this tool to be used in cross border cases?	Under the circumstances outlined in Chapter 4 Art. 28 of the ZeugSG, fedpol can transfer a person to be protected to a foreign country or take over a person to be protected from a foreign country. For persons for whom a witness protection program of a foreign state or an international criminal court is being carried out and who are brought to Switzerland for security reasons, the respective law outlined in ZeugSG shall apply insofar as an international treaty binding Switzerland does not contain any provisions to the contrary.	
What thresholds must be passed for the use of this tool?	There is no maximum term of imprisonment defined in this law. This law applies to persons who, by virtue of their cooperation or willingness to cooperate in federal or cantonal criminal proceedings, are or may be exposed to substantial danger to life or limb or to other serious disadvantage; and without whose cooperation the prosecution would have been disproportionately difficult or would have been disproportionately difficult.	Chapter 1 Art. 2 ZeugSG
What types of stakeholder are involved in the implementation of this tool?	Prosecutor, Witness Protection Unit, Federal Police. The witness protection unit is subordinate to fedpol. In terms of personnel and organisation, it is to be separated from the units conducting investigations.	ZeugSG
Which LEAs can use this tool?	Prosecutor	ZeugSG

Relevant items	Provisions	Sources used
What are the rules to be followed for the implementation of this tool?	- the person to be protected has to express his or her willingness to cooperate in the criminal proceedings Chapter 2 Art. 9 ZeugSG - authorisation procedure as outlined in Chapter 2 Art. 6-8 ZeugSG	• Chapter 2 Art. 6 ZeugSG • Chapter 2 Art. 6-8 ZeugSG • Chapter 2 Art. 9 ZeugSG
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	There are no specific restrictions to the use of the tool defined in ZeugSG	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	- The prosecutor may apply to the witness protection office for the implementation of a witness protection program. - The witness protection Unit conducts a comprehensive review process. Please refer to Chapter 2 Art. 7 for a list of criteria. - The director of The Federal office of Police (fedpol) decides on the implementation of a witness protection program at the request of the witness protection unit.	• Chapter 2 Art. 6-8 ZeugSG
What ongoing supervision is required for the use of this tool?	There is no ongoing supervision defined in the law related to a specific case. However, the Witness Protection Unit reports annually on its activities to the head of the Federal Department of Justice and Police (FDJP).	• Chapter 6 ZeugSG
Is there any national case law relating to the use of this tool in cross-border crime cases?	N/A	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	Eight witness protection cases were processed in 2018. Six cases were carried over from the previous year. In 2019, seven witness protection cases were processed. All seven cases were carried over from the previous year. Seven cases were processed in 2020. Six cases were carried over from the previous year.	• Report of the witness protection unit 2018: • https://www.fedpol.admin.ch/dam/fedpol/de/data/sicherheit/zeugenschutz/bericht_e/taetigkeitsbericht-zeugenschutzstelle-d.pdf.download.pdf/taetigkeitsbericht-zeugenschutzstelle-d.pdf • Report of the witness protection unit 2019: • https://www.fedpol.admin.ch/dam/fedpol/de/data/sicherheit/zeugenschutz/bericht_e/taetigkeitsbericht-zeugenschutzstelle-2019-d.pdf.download.pdf/taetigkeitsbericht-zeugenschutzstelle-2019-d.pdf • Report of the witness protection unit 2020: • https://www.fedpol.admin.ch/dam/fedpol/de/data/sicherheit/zeugenschutz/bericht_e/taetigkeitsbericht-zeugenschutzstelle-2020-d.pdf.download.pdf/taetigkeitsbericht-zeugenschutzstelle-2020-d.pdf
Surveillance		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Procedure Code (CCP) (Strafprozessordnung StPO) Federal Act of 18 March 2016 on the Surveillance of Post and Telecommunications (SPTA)	• Criminal Procedure Code (CCP) (Strafprozessordnung StPO) • https://www.fedlex.admin.ch/eli/cc/2010/267/en • Federal Act of 18 March 2016 on the Surveillance of Post and Telecommunications (SPTA) https://www.fedlex.admin.ch/eli/cc/2018/31/de
Specific range of application of the tool	- Post and Telecommunications Surveillance - Surveillance using Technical Surveillance Devices - Observation - Surveillance of Banking Transactions	• CCP Title 5 Chapter 8 Section 1 (Post and Telecommunications) • CCP Title 5 Chapter 8 Section 2 (Technical Surveillance Devices) • CCP Title 5 Chapter 8 Section 3 (Observation) • CCP Title 5 Chapter 8 Section 4 (Surveillance of Banking Transactions)
How is the tool defined?	Surveillance of Post and Telecommunications Monitoring of post and telecommunications of an accused person or third parties if there is reason to believe based on specific information that the accused uses the postal address or the telecommunications service of the third party, or the third party receives certain communications on behalf of the accused or passes on communications from the accused to another person. Technical Surveillance Devices: - listen to or record words spoken in private; - observe or record events in private or not generally accessible places; - establish the whereabouts of persons or property. Observation: covertly observe persons and property in generally accessible locations and make image or sound recordings while doing so Surveillance of Banking Transactions: In order to investigate felonies or misdemeanours, the compulsory measures court may, at the request of the public prosecutor, order the surveillance of transactions between a suspect and a bank or bank-type institution.	• Section 1 Art. 270 • Section 2 Art. 280 • Section 3 Art. 282 • Section 4 Art. 284
For what types of crime can the tool be used?	Cross crime areas. Surveillance may be ordered in the investigation of the offences under the Articles stated in Art. 269 paragraph 2 CCP	• Art. 269
Does national law allow this tool to be used in cross border cases?	The public prosecutor may arrange for post and telecommunications to be monitored if there is a strong suspicion that an offence listed in paragraph 2 has been committed; the seriousness of the offence justifies surveillance; and investigative activities carried out so far have been unsuccessful or the enquiries would otherwise have no prospect of success or be made unreasonably complicated.	• Art. 269 • Art. 282

Relevant items	Provisions	Sources used
	The public prosecutor and, in the enquiries, the police may covertly observe persons and property in generally accessible locations and make image or sound recordings while doing so if there is reason to believe on the basis of specific information that felonies or misdemeanours have been committed; and the enquiries would otherwise have no prospect of success or be made unreasonably complicated.	
What thresholds must be passed for the use of this tool?	LEAs, Federal Council for the use of special technical devices for surveillance of telecommunications	Art. 269bis
What types of stakeholder are involved in the implementation of this tool?	Criminal Police, Public Prosecution, Federal Council	- Art. 269 - Art. 269bis
Which LEAs can use this tool?	The surveillance of post and telecommunications requires the authorisation of the compulsory measures court.	Art. 274
What are the rules to be followed for the implementation of this tool?	The authorisation procedure is outlined in Art. 274 of the CCP. '- The public prosecutor shall submit the order and a statement of reasons and the case documents relevant for authorisation to the compulsory measures court within 24 hours of surveillance or the release of information being ordered. - The compulsory measures court shall decide and provide a brief statement of the reasons within 5 days of the surveillance or the release of information being ordered. It may grant authorisation subject to a time limit or other conditions, or request further information or investigations - The compulsory measures court shall give notice of the decision immediately to the public prosecutor and to the Post and Telecommunications Surveillance Bureau in terms of Article 3 SPTA - The authorisation shall expressly state which measures must be taken to protect professional confidentiality and whether non-public spaces may be entered in order to introduce special software into the relevant data processing system - The compulsory measures court shall grant authorisation for a maximum of 3 months. The authorisation may be extended on one or more occasions for a maximum of 3 months at a time. If an extension is required, the public prosecutor shall file an application for the extension, stating the reasons therefor, before expiry of the current authorisation. If enquiries reveal that the person under surveillance is changing his or her telecommunications service regularly, the compulsory measures court may by way of exception authorise the surveillance of all identified services used by the person under surveillance for telecommunications so that authorisation is not required in each individual case (general authorisation). The public prosecutor shall submit a report to the compulsory measures court for approval every month and on conclusion of the surveillance. If during the surveillance of a service in terms of a general authorisation, measures are required to protect professional confidentiality and such measures are not mentioned in the general authorisation, an application for authorisation for the individual surveillance operation concerned must be submitted to the compulsory measures court.	- Art. 274 - Art. 272 - Federal Act of 18 March 2016 on the Surveillance of Post and Telecommunications (SPTA) https://www.fedlex.admin.ch/eli/cc/2018/31/de
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	In monitoring postal and telecommunications traffic, the agency has the general responsibilities to give instructions to the parties obliged to cooperate on how to carry out the monitoring, asks them to take the necessary measures for the monitoring and controls the execution. Where observation activities ordered by the police have been conducted for one month, their continuation requires authorisation by the public prosecutor.	- Art. 16 SPTA - Art. 282
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	Date: 12 July 2012 Summary: The case concerns remote effect of the prohibition of the use of evidence. It was found that findings from unauthorised telephone surveillance are absolutely unusable. This also applies if the authorisations required under foreign law for telephone surveillance carried out abroad are missing.	- Official Collection of the Decisions of the Federal Tribunal" ("Amtliche Sammlung der Entscheidungen des schweizerischen Bundesgerichts (BGE) 138 IV 169 https://www.bger.ch/ext/eurospider/live/de/php/clir/http/index.php?lang=de&type=highlight_simple_query&page=1&from_date=&to_date=&from_year=2000&to_year=2021&sort=relevance&subcollection_c6=on&insertion_date=&from_date_push=&top_subcollection_clir=any&query_words=%FCberwachung+grenz%FCberschreitend&part=all&de_fr=&de_it=&fr_de=&fr_it=&it_de=&it_fr=&orig=&translation=&rank=1&highlight_docid=atf%3A%2F%2F138-IV-169%3Ade&number_of_ranks=34&aazacir=clir#idp376000
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	Criminal Procedure Code (CCP) (Strafprozessordnung StPO) Federal Act of 18 March 2016 on the Surveillance of Post and Telecommunications (SPTA)	- Criminal Procedure Code (CCP) (Strafprozessordnung StPO) https://www.fedlex.admin.ch/eli/cc/2010/267/en - Federal Act of 18 March 2016 on the Surveillance of Post and Telecommunications (SPTA) https://www.fedlex.admin.ch/eli/cc/2018/31/de
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	- Post and Telecommunications Surveillance - Surveillance using Technical Surveillance Devices - Observation - Surveillance of Banking Transactions	- CCP Title 5 Chapter 8 Section 1 (Post and Telecommunications) - CCP Title 5 Chapter 8 Section 2 (Technical Surveillance Devices) - CCP Title 5 Chapter 8 Section 3 (Observation) - CCP Title 5 Chapter 8 Section 4 (Surveillance of Banking Transactions)

Relevant items	Provisions	Sources used
Undercover / covert operations		
Relevant documents (legal and non-legal) that define the functioning of the tool	Criminal Procedure Code (CCP) (Strafprozessordnung StPO)	• SR 312.0 - Swiss Criminal Procedure Code of 5 October 2007 (Criminal Procedure Code, CCP) (admin.ch)
How is the tool defined?	Undercover Investigation: In an undercover investigation, police officers or persons temporarily appointed to carry out police duties make contact with persons under false pretences by using a false identity (cover) supported by documents with the aim of gaining the trust of those persons and infiltrating a criminal environment in order to investigate particularly serious offences. Undercover Enquiries: In undercover enquiries, police officers deployed for short periods in such a way that their true identity and function remains concealed attempt to investigate felonies and misdemeanours and to do so enter into or pretend that they wish to enter into fictitious transactions.	• Chapter 8 Section 5 (Undercover Investigations) • Chapter 8 Section 5a (Undercover Enquiries)
For what types of crime can the tool be used?	Cross crime areas. An undercover investigation is permitted in respect of offences under the Articles listed in Art. 286 paragraph 2 CCP	• Art. 286
Does national law allow this tool to be used in cross border cases?	Undercover investigation may be ordered if it is suspected that an offense listed in paragraph 2 of Art. 286 has been committed, the seriousness of the offence justifies the covert investigation and previous investigative activities have been unsuccessful or the enquiries would otherwise have no prospect of success or be made unreasonably complicated. Undercover enquiries may be ordered if it is suspected that a felony or misdemeanour has been committed and previous enquiries or investigations have been unsuccessful or the enquiries would otherwise have little prospect of success or would be made disproportionately more complex.	• Art. 286 • Art. 298b
What thresholds must be passed for the use of this tool?	LEAs	
What types of stakeholder are involved in the implementation of this tool?	Criminal Police, Public Prosecution The public prosecutor and, during police enquiries, the police may order undercover enquiries	• Art. 285a, Art. 286 • Art. 298b
Which LEAs can use this tool?	In Undercover Investigations, members of a Swiss or foreign police force and persons employed temporarily on police duties even if they have not received police training can be deployed. However, only members of a police force may be deployed as command staff. In Undercover Enquiries, only members of a Swiss or foreign police force can be deployed. The deployment of an undercover investigator requires the authorisation of the compulsory measures court.	• Art. 287 • Art. 298b • Art. 289
What are the rules to be followed for the implementation of this tool?	The authorisation procedure is outlined in Art. 289 of the CCP. '- The public prosecutor shall submit the order and a statement of reasons and the case documents relevant for authorisation to the compulsory measures court within 24 hours of ordering the undercover investigation. - The compulsory measures court shall decide and provide a brief statement of the reasons within 5 days of the undercover investigation being ordered. It may grant authorisation subject to a time limit or other conditions, or request further information or investigations - The authorisation shall expressly state specific permissions related to altered documents, guaranteed anonymity and the deployment of persons with no police training - The compulsory measures court shall grant authorisation for a maximum of 12 months. Authorisation may be extended on one or more occasions for a maximum of 6 months at a time. If an extension is required, the public prosecutor shall file an application for the extension, stating the reasons therefor, before expiry of the current authorisation. - If authorisation is not granted or no authorisation has been obtained, the public prosecutor shall terminate deployment immediately. All records must be destroyed immediately. Findings made by means of the undercover investigation may not be used. If undercover enquiries ordered by the police have been carried out for one month, the public prosecutor must approve their continuation.	• Art. 289 • Art. 298b
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	During deployment, the undercover investigator is subject to the direct instructions of the commanding officer. During deployment, any contact between the public prosecutor and the undercover investigator shall take place exclusively via the commanding officer. The commanding officer has the duty to brief the undercover investigator in detail and continuously on the assignment, to instruct and advise the undercover investigator, to continually assess the risk situation and to inform the public prosecutor regularly and in full on the operation	• Art. 291
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	

Relevant items	Provisions	Sources used
Is there any national case law relating to the use of this tool in cross-border crime cases?	Criminal Procedure Code (CCP) (Strafprozessordnung StPO)	• SR 312.0 - Swiss Criminal Procedure Code of 5 October 2007 (Criminal Procedure Code, CCP) (admin.ch)
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	Undercover Investigation: In an undercover investigation, police officers or persons temporarily appointed to carry out police duties make contact with persons under false pretences by using a false identity (cover) supported by documents with the aim of gaining the trust of those persons and infiltrating a criminal environment in order to investigate particularly serious offences. Undercover Enquiries: In undercover enquiries, police officers deployed for short periods in such a way that their true identity and function remains concealed attempt to investigate felonies and misdemeanours and to do so enter into or pretend that they wish to enter into fictitious transactions.	• Chapter 8 Section 5 (Undercover Investigations) • Chapter 8 Section 5a (Undercover Enquiries)
Use of informants		
Relevant documents (legal and non-legal) that define the functioning of the tool	Informants are not explicitly named by Swiss law.	
Specific range of application of the tool	N/A	
How is the tool defined?	N/A	
For what types of crime can the tool be used?	N/A	
Does national law allow this tool to be used in cross border cases?	N/A	
What thresholds must be passed for the use of this tool?	N/A	
What types of stakeholder are involved in the implementation of this tool?	N/A	
Which LEAs can use this tool?	N/A	
What are the rules to be followed for the implementation of this tool?	N/A	
Safeguards provided by national criminal laws to protect the rights of the individuals, ensure proportionality, and protect rule of law (if any)	N/A	
What authorisation is needed for the use of this tool (e.g. senior police officer, prosecutor, judge, other)?	N/A	
What ongoing supervision is required for the use of this tool?	N/A	
Is there any national case law relating to the use of this tool in cross-border crime cases?	Informants are not explicitly named by Swiss law.	
Is there any data available in your country on the number of times this tool has been used for organised crime cases? If yes can you please indicate the relevant statistics?	N/A	

Source: Author’s own elaboration

4 COVERAGE OF ISSUES BY THE SCHENGEN EVALUATION REPORTS

The table below provides an overview of the extent to which the issues identified in the report have been also reported in the Schengen Evaluation Reports (covering the period 2015-2019) that DG HOME shared with the Team.

Table 49 – Overview of the extent to which the issues identified in the report are also reported in the Schengen Evaluation Reports

Core problem	Drivers	C1	C3	C4	C5	C6	C8	C9	C10	C11	C12	C13	C15	C16	C17	C18	C19	C20	C21	C23	C24	C25	C27	C28	C29	C30	C31	Total	Share of countries
Access to and exchange of necessary information between law enforcement authorities is sub-optimal	Difficulties in the implementation of relevant EU provisions																												
	Some requirements set in the SFD are unclear and (unnecessarily) complex																											19	73%
	Uncertainties in the use of the proper legal basis																											7	27%
	Insufficient knowledge of existing mechanisms, skill gaps and outdated IT infrastructures																												
	National LEAs have limited awareness and knowledge of relevant databases																											24	92%
	Limited offer of training that is focused on cross-border law enforcement cooperation																											20	77%
	Language barriers hamper the cross-border exchange of information																											12	46%
	Use of rudimentary search tools hampers the adoption of transliteration and "fuzzy logic" search																											13	50%
	Differences in national implementation choices																												
	SPOCs do not always play their coordination role and lack resources to face the increasing number of requests																											7	27%
	Differences in access rights and use EU of and international databases and platforms between national law enforcement authorities																											21	81%
	EU intelligence picture does not fully reflect the cross-border dimension of security threats																												
	National specialised analytical departments rarely cooperate with similar departments in other countries to conduct cross-border threat assessments																											11	42%
	Limited exchange of information between national law enforcement agencies																											22	85%
Total		3	9	5	3	8	6	8	5	5	5	5	3	5	7	5	7	5	4	3	9	6	6	10	4	6	6	148	

Core problem	Drivers	C1	C3	C4	C5	C6	C8	C9	C10	C11	C12	C13	C15	C16	C17	C18	C19	C20	C21	C23	C24	C25	C27	C28	C29	C30	C31	Total	Share of countries
Too few joint operations for public order and safety purposes are taking place	Limited executive powers of police officers operating in the respective host States ⁸																											0	0%
	Lack of interoperability of radio telecommunication equipment																											23	88%
	Limited remote access to law enforcement databases																											16	62%
	Total	2	2	1	2	2	1	2	2	1	0	1	2	1	0	2	2	1	0	1	2	2	2	2	2	2	2	2	39
EU and national implementation rules hamper cross-border operational cooperation to fight SOC	Bi/tri/multilateral agreements create a complex web of different rules and standards																											11	42%
	Limited relevance of EU legal provisions on cross-border hot-pursuit and surveillance																											6	23%
	National rules for cross-border controlled deliveries, surveillance and hot pursuit are not consistent																											22	85%
	Total	2	2	2	1	2	2	1	2	2	1	2	2	0	1	3	1	2	1	1	1	1	2	2	1	2	0	1	39
Total		7	13	8	6	12	9	11	9	8	6	8	7	6	8	10	10	8	5	5	12	10	10	13	8	8	9	226	

Source: Author’s own elaboration based on the Schengen Evaluation Reports

⁸ The Team did not find any evidence stemming from the Schengen Evaluation Reports supporting this driver.

5 CONSULTATION TOOLS AND STAKEHOLDERS ENGAGED

5.1 Consultation tools

Survey questionnaire for LEAs

Table 50 – Survey questionnaire for LEAs

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
1	PERSONAL INFORMATION		Your first name*	open text	x	x	x	x	x	x	x	x
2	PERSONAL INFORMATION		Your last name*	open text	x	x	x	x	x	x	x	x
3	PERSONAL INFORMATION		Name of the organisation you belong to*	open text	x	x	x	x	x	x	x	x
4	PERSONAL INFORMATION		Your role*									
5	PERSONAL INFORMATION		Your email address*	open text	x	x	x	x	x	x	x	x
6	PERSONAL INFORMATION		Your country*	Drop down list of 27 + Schengen	x	x	x	x	x	x	x	x
7	THREAT LANDSCAPE	Challenges related to SOC	To what extent has the number of crimes evolved in the past 5-10 years in the following areas in your country?*	*Drugs *Illicit tobacco trade *Trafficking in human beings *Financial crimes *Cybercrime *Organised property crime *Environmental crime *Trafficking of firearms *Illegal immigration *Terrorism *Other (please specify)	x	x	x	x		x	x	x
8	THREAT LANDSCAPE	Challenges related to SOC	Can you please provide some figures related to crimes occurred over the past 5-10 years or indicate where we could find them?	open text	x	x	x	x		x	x	x
9	THREAT LANDSCAPE	Challenges related to SOC	In your view, to what extent do the following crime areas have a cross border dimension (i.e. require the EU-wide cooperation of law enforcement authorities to be properly addressed)?*	*Drugs *Illicit tobacco trade *Trafficking in human beings *Financial crimes *Cybercrime *Organised property crime *Environmental crime *Trafficking of firearms *Illegal immigration *Terrorism	x	x	x	x		x	x	x
9.A	THREAT LANDSCAPE	Challenges related to SOC	Could you please specify any other relevant crime area which you think it has a cross border dimension?		x	x	x	x		x	x	x
10	THREAT LANDSCAPE	Challenges related to SOC	How do you think the crime areas listed below will evolve over the next 5-10 years in your country?*	*Drugs *Illicit tobacco trade *Trafficking in human beings *Financial crimes *Cybercrime *Organised property crime *Environmental crime *Trafficking of firearms *Illegal immigration	x	x	x	x		x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
				*Terrorism *Other (please specify)								
11	THREAT LANDSCAPE	Challenges related to the security of EU citizens moving across the EU	In your view, how has the number of accidents linked to public order and safety evolved over the past 5-10 years in your country in the following areas?*	*International sport/music/cultural events *Flows of people moving for tourism *Flows of people moving for work	x	x	x	x	x	x	x	x
12	THREAT LANDSCAPE	Challenges related to the security of EU citizens moving across the EU	Can you please provide some figures related to accidents occurred over the past 5-10 years or indicate where we could find them?	open text	x	x	x	x	x	x	x	x
13	THREAT LANDSCAPE	Challenges related to the security of EU citizens moving across the EU	In your view, to what extent do the following areas require cross-border law enforcement cooperation (i.e. require the EU-wide cooperation of law enforcement authorities to be properly managed)?*	*International sport/music/cultural events *Flows of people moving for tourism *Flows of people moving for work	x	x	x	x	x	x	x	x
13.A	THREAT LANDSCAPE	Challenges related to the security of EU citizens moving across the EU	Can you please specify any other type of event or activity which requires cross-border law enforcement cooperation in the area of public safety and/or public order?		x	x	x	x	x	x	x	x
14	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation SOC	How often do law enforcement authorities in your country undertake operational cooperation with law enforcement authorities in other countries in relation to the following crimes?*	*Drugs *Illicit tobacco trade *Trafficking in human beings *Financial crimes *Cybercrime *Organised property crime *Environmental crime *Trafficking of firearms *Illegal immigration *Terrorism	x		x			x	x	x
15	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation SOC	Out of all cases where your country undertook operational cooperation with other countries in relation to serious and organised crimes, what was the share of problematic cases?*	*Never had problematic cases *0-20% *20-40% *40-60% *60-80% *80-100% *All cases were problematic	x		x			x	x	x
16	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation SOC	What were the main reasons for the difficulties encountered?	*lack of clarity on the rules to be followed *missing or unclear points of contact *time delays *language barriers *different rules applicable to the same criminal act and investigative tools in the other country *high number of administrative requirements to comply with *lack of trust *other (please specify)	x		x			x	x	x
17	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation SOC	What were the main consequences of the difficulties encountered?	*Increase of time needed for the investigations *Costs for complying with unexpected requirements *Impossibility to continue the	x		x			x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
				investigation/case *Other (please specify)								
18	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation SOC	If difficulties encountered brought to time delays, can you please estimate these delays?	* 1-7 days * 2-4 weeks *2-3 months *More than 3 months *Don't know	x		x			x	x	x
19	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation SOC	If difficulties encountered brought to additional costs, can you please indicate the type of costs?	*Costs related to additional staff needed *Costs related to the compliance with unexpected requirements of the other country *Costs related to the purchase of new equipment *Other costs (please specify)	x		x			x	x	x
20	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation Public Order	How often do law enforcement authorities in your country undertake operational cooperation with law enforcement authorities in other countries to ensure public order and safety?*	*Crises and disasters *International sport/music/cultural events *Flows of people moving for tourism *Flows of people moving for work *Protection of public figures	x	x			x	x	x	x
20.A	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation Public Order	Do you have any other relevant example of events or activities for which your country undertake operational cooperation with law enforcement authorities in other countries to ensure public order and safety?		x	x			x	x	x	x
21	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation Public Order	Out of all cases where your country undertook operational cooperation with other countries to ensure public order and safety, what was the share of problematic cases?*	*Never had problematic cases *0-20% *20-40% *40-60% *70-80% *80-100% *All cases were problematic	x	x			x	x	x	x
22	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation Public Order	What were the main reasons for the difficulties encountered?	*Lack of clarity on the rules to be followed *Missing or unclear points of contact *Time delays *Language barriers *Different rules applicable to the same criminal act and investigative tools in the other country *High number of administrative requirements to comply with *Lack of trust *Other (please specify;	x	x			x	x	x	x
23	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation Public Order	What were the main consequences of the difficulties encountered?	*Increase of time needed for the operation *Costs for complying with unexpected requirements *Impossibility to continue the operation *Other (please specify)	x	x			x	x	x	x
24	THE CURRENT EU FRAMEWORK FOR LAW	Operational cooperation Public Order	If difficulties encountered brought to time delays, can you please estimate these delays?	* 1-7 days * 2-4 weeks *2-3 months	x	x			x	x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
	ENFORCEMENT COOPERATION			*More than 3 months *Don't know								
25	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation Public Order	If difficulties encountered brought to additional costs, can you please indicate the type of costs?	*Costs related to additional staff needed *Costs related to the compliance with unexpected requirements of the other country *Costs related to the purchase of new equipment *Other costs (please specify)	x	x			x	x	x	x
26	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation - structures	To what degree do you use the following structures to cooperate with other law enforcement authorities in other countries?*	*Single Points of Contact (SPOCs) *Police Customs Cooperation Centres (PCCCs) *National SIRENE Bureaux *Europol National Units *Europol Liaison Officers *Football Points of Contact	x	x	x		x	x	x	x
27	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation - structures	Please list any other structures, not listed in the question above, that you use to facilitate cooperation with law enforcement authorities in other countries?	open text	x	x	x		x	x	x	x
28	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation - structures	To what degree are the following structures effective in facilitating cross border cooperation between law enforcement authorities in your country and law enforcement authorities in other countries?*	*Single Points of Contact (SPOCs) *Police Customs Cooperation Centres (PCCCs) *National SIRENE Bureaux *Europol National Units *Europol Liaison Officers *Football Points of contact	x	x	x		x	x	x	x
29	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation - structures	To what degree do the following issues hamper cross border law enforcement cooperation using the structures listed above?*	*Confusion caused by the number of different points of contact in the countries (for example, liaison officers, Single Points Of Contacts - SPOCs, SIRENE Bureaux, ENUs, Police Customs Cooperation Centres - PCCCs, SIRENE Bureaux etc.) *Differences between countries in the way that SPOCs are structured *SPOCs and PCCCs are not coordinated *Law enforcement practitioners are not aware of factsheets and manuals explaining the different roles and responsibilities *Factsheets and manuals providing implementation guidance are not kept up to date/are not clear, precise, committal enough to ensure proper implementation? *Lack of communication and coordination between different law enforcement authorities within countries *Lack of coordination between law enforcement and judicial authorities within countries *Lack of coordination between policing and customs authorities within countries	x	x	x		x	x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
				*Developments in relation to customs cooperation have occurred in parallel to the EU legal framework for law enforcement cooperation thus creating risks of duplications, inconsistencies and inefficiencies in operational situations								
30	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Operational cooperation - structures	Please provide further information and examples to illustrate the issues that hamper the use of the structures listed above.	open text	x	x	x		x	x	x	x
31	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Information exchange	How often do law enforcement authorities in your country undertake information sharing with law enforcement authorities in other countries in relation to the following criminal threats?*	*Drugs *Illicit tobacco trade *Trafficking in human beings *Financial crimes *Cybercrime *Organised property crime *Environmental crime *Trafficking of firearms *Illegal immigration *Terrorism	x	x	x		x	x	x	x
32	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Information exchange	How often do law enforcement authorities in your country undertake information sharing with law enforcement authorities in other countries for public order purposes?*	*Crises and disasters *International sport/music/cultural events *Flows of people moving for tourism *Flows of people moving for work *Protection of public figures *Other (please specify)	x	x	x		x	x	x	x
33	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Information exchange	Out of all cases where your country shared information with other countries, what was the share of problematic cases?*	*Never had problematic cases *0-20% *20-40% *40-60% *60-80% *80-100% *All cases were problematic	x	x	x		x	x	x	x
34	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Information exchange	What were the main reasons for the difficulties encountered?	*unclear rules to be followed *missing or unclear points of contact *time delays *language barriers *inadequate tools for the exchange of sensitive/confidential information *high number of administrative requirement to comply with *lack of trust *other (please specify)	x	x	x		x	x	x	x
35	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Information exchange	What were the main consequences of the difficulties encountered?	*Increase of time needed for the investigations/acquisition of intelligence *Costs for complying with unexpected requirements *Impossibility to continue the investigation/case *Other (please specify)	x	x	x		x	x	x	x
36	THE CURRENT EU FRAMEWORK FOR LAW	Information exchange	If difficulties encountered brought to time delays, can you please estimate these delays?	* 1-7 days * 2-4 weeks *2-3 months	x	x	x		x	x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
	ENFORCEMENT COOPERATION			*More than 3 months *Don't know								
37	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Information exchange	If difficulties encountered brought to additional costs, can you please indicate the type of costs?	*Costs related to additional staff needed *Costs related to the compliance with unexpected requirements of the other countries *Costs related to the purchase of new equipment *Other costs (please specify)	x	x	x		x	x	x	x
38	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Information exchange - platforms	To what degree do you use the following platforms to exchange information with law enforcement authorities in other countries?*	*SIENA *Schengen Information System (SIS))/SIRENE *Europol Information System (EIS) *Interpol exchange channels and databases	x	x	x		x	x	x	x
39	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Information exchange - platforms	Please list any other platforms, not listed in the question above, that you use to exchange information with law enforcement authorities in other countries	open text	x	x	x		x	x	x	x
40	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Information exchange - platforms	To what degree are the following platforms effective in facilitating the exchange of information among law enforcement authorities in different countries?*	*SIENA *Schengen Information System (SIS))/SIRENE *Europol Information System (EIS) *Interpol exchange channels and databases	x	x	x		x	x	x	x
41	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Information exchange - platforms	To what degree do the following issues hamper cross border law enforcement cooperation through the platforms listed above?*	*The EU legal framework for cross-border law enforcement cooperation is not consolidated (i.e. it is spread across several legislative instruments) *Council guideline papers on info exchange are found not clear, precise and complete enough to offer added value in the implementation of the EU texts *The complexity (overlaps, discrepancies, gaps) in the EU legal framework for information exchange *The EU legal framework for cross-border law enforcement cooperation is not consistently implemented across the countries (i.e. the countries implement it differently) *Access to these platforms differs between countries *Differences between countries in how regularly these platforms are monitored/ response times to requests sent via these platforms *Heterogeneity in law enforcement actors, tools, and capacities in relation to cross-border cooperation creates confusion and burdens on the concerned stakeholders	x	x	x		x	x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
				*Confusion due to the number of different exchange platforms and databases for EU information exchange *Data protection requirements limit exchange of information with law enforcement authorities in other countries								
42	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Information exchange - platforms	Please provide further information and examples to explain your answers about the issues that hamper the use of the platforms for exchange of information listed	open text	x	x	x		x	x	x	x
43	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Cross-border threat assessment/risk analysis	How often do you/your department undertake cross-border threat assessment/risk analysis?*	*Always *Very frequently *Occasionally *Very infrequently *Never *Don't know				x				
44	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Cross-border threat assessment/risk analysis	What were the main reasons for undertaking cross-border threat assessment/risk analysis?	*To feed the design of national law enforcement strategies and actions *To plan joint operations/patrols *To regularly update the national intelligence picture *Other (please specify)				x				
45	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Cross-border threat assessment/risk analysis	If you/your department undertake cross-border threat assessment/risk analysis, are these elaborated with other relevant national stakeholders?	*Yes *No *Don't know				x				
46	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Cross-border threat assessment/risk analysis	If yes, what type stakeholders? (select all that apply)	*Police *Customs *Financial Investigation Units *Other (please specify)				x				
47	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Cross-border threat assessment/risk analysis	Does your department involve stakeholders from other concerned countries in the implementation of cross-border threat assessments/risk analysis?	*Yes *No *Don't know				x				
48	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Cross-border threat assessment/risk analysis	If yes, what type stakeholders in the other countries are usually involved in cross-border threat assessments/risk analysis? (select all that apply)	*Single Points of Contacts *Police Customs Cooperation Centres *Specialised investigation units *Specialised analytical departments *Public safety/order specialists (especially the ones (who have been) involved in joint patrols, joint operations) *Football contact points *Customs *Other (please specify)				x				
49	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Cross-border threat assessment/risk analysis	Are cross-border threat assessment/risk analysis shared with the neighbouring country(ies) in view of joint analytical documents?*	*Yes *No *Don't know				x				

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
50	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Cross-border threat assessment/risk analysis	If yes, with which country(ies)?	open text				x				
51	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Cross-border threat assessment/risk analysis	Can cross-border threat assessment/risk analysis be used to schedule the precise location and timing of joint operations?*	*Yes *No *Don't know				x				
52	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Cross-border threat assessment/risk analysis	If not, why?	open text				x				
53	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Cross-border threat assessment/risk analysis	Can you please shortly describe how cross-border threat assessments/risk analysis is implemented? (e.g. type of information requested, types of analysis performed)	open text				x				
54	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Cross-border threat assessment/risk analysis	Out of all cases where you/your department undertook cross-border threat assessment/risk analysis, what was the share of problematic cases?	*Never had problematic cases *0-20% *20-40% *40-60% *60-80% *80-100% *All cases were problematic				x				
55	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Cross-border threat assessment/risk analysis	What were the main reasons for the difficulties encountered?	open text				x				
56	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Investigative tools for cross border crimes	How often are the following investigative tools used in cross-border investigations involving cooperation between law enforcement authorities in your country and those in other countries?*	*Cross border surveillance (physical) *Interception of communication *Covert investigations - undercover officers *Controlled deliveries *Informants *Hot pursuit *Special intervention units *Joint Patrols *Joint Police Offices *Witness protection	x	x	x			x	x	x
57	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Investigative tools for cross border crimes	What other investigative tools, not listed above, are used in cross-border investigations involving cooperation between law enforcement authorities in your country and those in other countries?	open text	x	x	x			x	x	x
58	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Investigative tools for cross border crimes	To what degree are the following tools effective in generating intelligence and evidence and/ or leading to the disruption of crimes in cross-border investigations involving cooperation between law enforcement authorities in your country and those in other countries?*	*Cross border surveillance (physical) *Interception of communication *Covert investigations - undercover officers *Controlled deliveries *Informants *Hot pursuit *Special intervention units *Joint Patrols	x	x	x			x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
				*Joint Police Offices *Witness protection								
59	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Investigative tools for cross border crimes	To what degree do the following act as barriers to the effective use of the investigative tools listed above in cross border cases?*	*Differences in national legislation regarding the offences for which an investigative tool may be authorised *Differences in national definitions regarding the length of time for which a special investigative tool may be authorised/ regularity of review *Other differences in national legislation regarding definition and scope of investigative tools *Financial costs of conducting cross-border operations utilising special investigative tools *Differences between countries in technologies (for example, different communications systems, different surveillance technologies) *Challenges in trust between countries *Restrictions on the ability to use investigative tools due to data protection regulations *Restrictions on the ability to use investigative tools due to fundamental rights protections *Lack of knowledge and training among law enforcement practitioners about how to apply for or implement investigative tools	x	x	x			x	x	x
60	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	Investigative tools for cross border crimes	Please provide further details to explain your answers above and to illustrate concrete examples of barriers to use of investigative tools in cross border cases.	open text	x	x	x			x	x	x
61	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	General	To what degree does the EU legal framework provide the necessary mechanisms for law enforcement authorities in your country to cooperate with other countries?*	*Schengen acquis - 1990 Convention implementing the Schengen Agreement of 1985 (CISA) *Swedish Framework Decision (Council Framework Decision 2006/960) *Naples II Convention (1998) *Prüm Decision (Council Decision 2008/615/JHA) *Council Decision 2007/412/JHA concerning security in connection with football matches with an international dimension *Council Decision 2006/560/JHA of 24 July 2006 on the common use of liaison officers posted abroad by the law enforcement agencies of the Member States	x	x	x		x	x	x	x
62	THE CURRENT EU FRAMEWORK FOR LAW	General	Has your country adopted other measures to enable cross border cooperation besides	*Yes *No *Don't know	x	x	x		x	x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
	ENFORCEMENT COOPERATION		those provided by the EU legal framework?*									
63	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	General	If yes, why?	*The EU legal Framework does not properly address the needs of my country *The EU legal framework is too complex and difficult to implement *It is easier to use measures and practices which stem from a national strategy than those offered by the EU framework *Other (please specify)	x	x	x		x	x	x	x
64	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	General	To what degree are the following non-binding documents useful to ensure the proper implementation of the Swedish Framework Decision, the Schengen acquis (CISA Convention), Prüm decision on joint operations and other documents they refer to?*	*Updated Catalogue of Recommendations for the correct application of the Schengen Acquis and Best practices: Police cooperation (15785/3/10); *Guidelines on the implementation of the Swedish Framework Decision (13034/14); *Draft Guidelines for a Single Point of Contact (SPOC) for international law enforcement information exchange (10492/14); *Manual on cross border operations (13887/20) and its National Factsheets (13920/20); *Manual on Law Enforcement Information Exchange (5825/20)	X	X	X		X	X	X	X
65	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	General	Can you please explain your previous assessment and indicate aspects of the documents that require improvement	open text	X	X	X		X	X	X	X
64.A	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	General	Do you have any other example of Council guideline papers of relevance? Please specify.		X	X	X		X	X	X	X
66	THE CURRENT EU FRAMEWORK FOR LAW ENFORCEMENT COOPERATION	General	Do you see additional barriers (not already listed above) to cross border law enforcement cooperation and to the effective use of investigative tools in cross border cases? If yes please specify	open text	x	x	x		X	x	x	x
67	MULTILATERAL AGREEMENTS	Number and type	Has your country entered into any bi/tri/multilateral agreements regarding law enforcement operational cooperation or information exchange with law enforcement authorities in other countries?*	*Yes *No *Don't know	x	x						x
68	MULTILATERAL AGREEMENTS	Number and type	If so, how many separate agreements has your country entered into?	1 2 3 4 5-10 More than 10 I don't know	x	x						x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
69	MULTILATERAL AGREEMENTS	Number and type	What type of stakeholders are involved in the implementation of these agreements?	*Only police *Only customs *Police and customs *I don't know *Other, please specify	x	x						x
70	MULTILATERAL AGREEMENTS	Number and type	Can you please list the agreements and provide the reference to the legal documents?	open text	x	x						x
71	MULTILATERAL AGREEMENTS	Number and type	How frequently or infrequently are these bi/tri/multilateral agreements used in practice?	*Very frequently (used in the majority of cross-border investigations with the signatory countries) *Occasionally (used in some cross border investigations) *Very infrequently (used in a small minority of cross border investigations) *Never *Don't know	x	x						x
72	MULTILATERAL AGREEMENTS	Scope and objectives	What was the reason your country decided to enter in the bi/tri/multilateral agreements?	open text	x	x						x
73	MULTILATERAL AGREEMENTS	Scope and objectives	What value did it add above existing EU and national frameworks facilitating cross border cooperation?	open text	x	x						x
74	MULTILATERAL AGREEMENTS	Scope and objectives	Are the following included in the bi/tri/multilateral agreements that your country has entered into?	*Information sharing *Joint Patrols *Joint offices or joint Units *Hot (cross-border) pursuit *Cross border surveillance *Joint threat assessment/risk analyses in view of tailored joint operations *Communications *Access to national databases *Competence/ authority on transport networks *Joint training *Authority to exercise police powers in another MS	x	x						x
74.A	MULTILATERAL AGREEMENTS	Scope and objectives	Is there any additional feature of the bi/tri/multilateral agreements that your country has entered into that was not listed above? Please specify.		x	x						x
75	MULTILATERAL AGREEMENTS	Good practices and areas for improvement	To what extent are these bi/tri/multilateral agreements effective in facilitating cross border cooperation between law enforcement authorities in your country and law enforcement authorities in other countries?	Very high extent High extent Moderate extent Small extent Not at all Don't know	x	x						x
76	MULTILATERAL AGREEMENTS	Good practices and areas for improvement	To what extent do you agree with the following statements about the bi/tri/multilateral agreements that your country has entered into?	*In my country there are too many bi/tri/multilateral agreements, causing complexity *The bi/tri/multilateral agreements are outdated *The bi/tri/multilateral agreements should be used more	x	x						x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
				*The bi/tri/multilateral agreements are procedurally heavy *The bi/tri/multilateral agreements do not provide the powers needed for effective cross border cooperation *Overall, the bi/tri/multilateral agreements work well *These agreements do not cover joint threat assessment/risk analyses in view of tailored joint operations; *When agreements provide for joint threat assessment/risk analyses, they are not been used in practice.								
77	MULTILATERAL AGREEMENTS	Good practices and areas for improvement	Are there any aspects of the bi/tri/multilateral agreements that your country is part on which you would recommend as good practice to other countries?	open text	x	x						x
78	INVESTIGATIVE TOOLS USED AT THE NATIONAL LEVEL TO COMBAT ORGANISED CRIME	Tools in use	How frequently do law enforcement authorities in your country use the following investigative tools to investigate serious and organised crime at the national level?*	*Controlled delivery (i.e. allowing suspicious shipments or cargo to leave, pass through or enter a jurisdiction with the knowledge and supervision of authorities) *Hot pursuit *Surveillance – Audio surveillance (e.g. Phone tapping; VOIP; Listening devices) *Surveillance – Visual surveillance (e.g. Hidden video-surveillance devices; body-worn video devices ; CCTV) *Surveillance – Tracking surveillance (e.g. GPS/transponders; mobile phones; radio-frequency identification devices (RFID); biometric info technology) *Surveillance – Data surveillance (e.g. computer/internet (spyware); mobile phones; keystroke monitoring) *Undercover operations *Use of informants – Members of the public *Use of informants – Victim of a crime *Use of informants – Members of an Organised Crime Group (OCG) *Use of informants – Other police officers *Witness protection	x	x	x			x	x	x
79	INVESTIGATIVE TOOLS USED AT THE NATIONAL LEVEL TO COMBAT ORGANISED CRIME	Tools in use	In what crime areas are the following tools used in your country?*	*Controlled delivery (i.e. allowing suspicious shipments or cargo to leave, pass through or enter a jurisdiction with the knowledge and supervision of authorities) *Hot pursuit	x	x	x			x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
				*Surveillance – Audio surveillance (e.g. Phone tapping; VOIP; Listening devices) *Surveillance – Visual surveillance (e.g. Hidden video-surveillance devices; body-worn video devices ; CCTV) *Surveillance – Tracking surveillance (e.g. GPS/transponders; mobile phones; radio-frequency identification devices (RFID); biometric info technology) *Surveillance – Data surveillance (e.g. computer/internet (spyware); mobile phones; keystroke monitoring) *Undercover/covert operations *Use of informants – Members of the public *Use of informants – Victim of a crime *Use of informants – Members of an Organised Crime Group (OCG) *Use of informants – Other police officers *Witness protection								
80	INVESTIGATIVE TOOLS USED AT THE NATIONAL LEVEL TO COMBAT ORGANISED CRIME	Tools in use	What types of measures are required to implement the following investigative tools across borders?*	*Controlled delivery (i.e. allowing suspicious shipments or cargo to leave, pass through or enter a jurisdiction with the knowledge and supervision of authorities) *Hot pursuit *Surveillance – Audio surveillance (e.g. Phone tapping; VOIP; Listening devices) *Surveillance – Visual surveillance (e.g. Hidden video-surveillance devices; body-worn video devices ; CCTV) *Surveillance – Tracking surveillance (e.g. GPS/transponders; mobile phones; radio-frequency identification devices (RFID); biometric info technology) *Surveillance – Data surveillance (e.g. computer/internet (spyware); mobile phones; keystroke monitoring) *Undercover/covert operations *Use of informants – Members of the public *Use of informants – Victim of a crime *Use of informants – Members of an Organised Crime Group (OCG) *Use of informants – Other police officers *Witness protection	x	x	x			x	x	x
81	INVESTIGATIVE TOOLS USED AT	Tools in use	Please list any investigative tools, not listed in the previous	open text	x	x	x			x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
	THE NATIONAL LEVEL TO COMBAT ORGANISED CRIME		question, which are allowed and used in your country to tackle serious and organised crime at the national level and specify for what crime area they are used									
82	INVESTIGATIVE TOOLS USED AT THE NATIONAL LEVEL TO COMBAT ORGANISED CRIME	Tools in use	Can you please indicate relevant national documents where the tools and the related applicable rules are described?	open text	x	x	x			x	x	x
83	INVESTIGATIVE TOOLS USED AT THE NATIONAL LEVEL TO COMBAT ORGANISED CRIME	Effectiveness of tools	To what degree do you consider the following tools to be effective in combating organised crime or other serious crimes when investigating organised crime groups?*	*Controlled delivery (i.e. allowing suspicious shipments or cargo to leave, pass through or enter a jurisdiction with the knowledge and supervision of authorities) *Hot pursuit *Surveillance – Audio surveillance (e.g. Phone tapping; VOIP; Listening devices) *Surveillance – Visual surveillance (e.g. Hidden video-surveillance devices; body-worn video devices ; CCTV) *Surveillance – Tracking surveillance (e.g. GPS/transponders; mobile phones; radio-frequency identification devices (RFID); biometric info technology) *Surveillance – Data surveillance (e.g. computer/internet (spyware); mobile phones; keystroke monitoring) *Undercover/covert operations *Use of informants – Members of the public *Use of informants – Victim of a crime *Use of informants – Members of an Organised Crime Group (OCG) *Use of informants – Other police officers *Witness protection	x	x	x			x	x	x
84	INVESTIGATIVE TOOLS USED AT THE NATIONAL LEVEL TO COMBAT ORGANISED CRIME	Effectiveness of tools	Are there any investigative tools currently available in your country that you would like to change - if so, how?	open text	x	x	x			x	x	x
85	INVESTIGATIVE TOOLS USED AT THE NATIONAL LEVEL TO COMBAT ORGANISED CRIME	Effectiveness of tools	Are there any investigative tools NOT currently available in your country that you would like to be able to use?	open text	x	x	x			x	x	x
86	INVESTIGATIVE TOOLS USED AT THE NATIONAL LEVEL TO COMBAT	Effectiveness of tools	Do you consider existing national safeguards as appropriate to protect the rights of the individuals when	*Yes *No *Don't know	x	x	x			x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
	ORGANISED CRIME		using the investigative tools listed above?*									
87	INVESTIGATIVE TOOLS USED AT THE NATIONAL LEVEL TO COMBAT ORGANISED CRIME	Effectiveness of tools	If not, can you please explain why?	open text	x	x	x			x	x	x
88	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Need for EU Action	To what extent, in your view, is there a need for EU intervention to improve cross-border law enforcement operational cooperation to the following types of crimes?*	*Drugs *Illicit tobacco trade *Trafficking in human beings *Financial crimes *Cybercrime *Organised property crime *Environmental crime *Trafficking of firearms *Illegal immigration *Terrorism	x		x			x	x	x
89	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Need for EU Action	To what extent, in your view, is there a need for EU intervention to improve cross-border law enforcement operational cooperation to ensure public order and safety?*	*Crises and disasters *International sport/music/cultural events *Flows of people moving for tourism *Flows of people moving for work *Protection of public figures	x	x			x	x	x	x
90	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Need for EU Action	To what extent, in your view, is there a need for EU intervention to improve cross-border information exchange among law enforcement authorities?*	Very high extent High extent Moderate extent Small extent Not at all Don't know	x	x	x		x	x	x	x
91	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Need for EU Action	To what extent, in your view, is there a need for EU intervention to improve cross-border threat assessment/risk analysis?*	Very high extent High extent Moderate extent Small extent Not at all Don't know				x				
92	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Need for EU Action	If you see the need for EU intervention, can you please explain what would be the added value of the intervention compared to what countries could achieve alone?	open text	x	x	x	x	x	x	x	x
93	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Policy Options	What type of measures the EU can adopt to improve cross-border threat assessment/risk analysis?	open text				x				
94	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Policy Options	To what extent do you think the following options can contribute to improving cross-border law enforcement cooperation between countries?*	*Consolidation, streamlining and clarification of the EU legal framework providing the basis for law enforcement cooperation *Modernisation of the EU legal framework providing the basis for law enforcement cooperation (e.g. by providing provisions to cover the use of recent technological developments) *Definition of minimum EU standards for organised crime investigations *Creation of a single set of rules for the same actions, whether	x	x	x		x	x	x	x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
				carried out by the police or by customs authorities *Setting up new operational initiatives for law enforcement cooperation *Design of new recommendations, guidelines and good practices for law enforcement cooperation								
95	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Policy Options	Please provide further details to explain your answer	open text	x	x	x		x	x	x	x
96	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Policy Options	Please list any other changes or steps do you think should be taken to improve cross-border law enforcement cooperation between countries	open text	x	x	x		x	x	x	x
97	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Policy Options	To what extent do you think EU intervention to harmonise the definitions and procedures relating to the following investigative tools would improve cross border cooperation?*	*Controlled delivery (i.e. allowing suspicious shipments or cargo to leave, pass through or enter a jurisdiction with the knowledge and supervision of authorities) *Hot pursuit *Surveillance – Audio surveillance (e.g. Phone tapping; VOIP; Listening devices) *Surveillance – Visual surveillance (e.g. Hidden video-surveillance devices; body-worn video devices ; CCTV) *Surveillance – Tracking surveillance (e.g. GPS/transponders; mobile phones; radio-frequency identification devices (RFID); biometric info technology) *Surveillance – Data surveillance (e.g. computer/internet (spyware); mobile phones; keystroke monitoring) *Undercover/covert operations *Use of informants – Members of the public *Use of informants – Victim of a crime *Use of informants – Members of an Organised Crime Group (OCG) *Use of informants – Other police officers *Witness protection	x	x	x			x	x	x
98	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Policy Options	Please provide further details to explain your answer	open text	x	x	x			x	x	x
99	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Policy Options	Please list any other investigative tools you think should have common definitions or approaches at the EU level?	open text	x	x	x			x	x	x
100	NEED FOR EU ACTION AND	Need for EU Action	To what extent do you think there is a need for EU action to harmonise and standardise the		x	x						x

N	Section	Sub-section	Question	Response options	SPOCs	PCCCs	Specialised investigation units	Specialised analytical departments	Public safety/ order specialists and Football Points of contact	Customs	Other National LEAs	NEC
	POSSIBLE SOLUTIONS		cooperation measures and standards currently included in bi/tri/multilateral agreements?*									
101	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Need for EU Action	Please provide further details to explain your answer	open text	x	x						x
102	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Policy Options	EU action might bring law enforcement authorities in your country to get additional powers. To what extent do you think this requires additional safeguards to be adopted in your country?*		x	x	x		x	x	x	x
103	NEED FOR EU ACTION AND POSSIBLE SOLUTIONS	Policy Options	Could you please illustrate the types of safeguards that you think should be adopted?	open text	x	x	x		x	x	x	x
104		General	Please include any additional contribution you would like to make to the study	open text	x	x	x	x	x	x	x	x
105		General	Would you like to be involved in the next consultation activities related to this study (interviews and focus groups)?*	*Yes *No	x	x	x	x	x	x	x	x
					94	87	72	32	50	80	80	94

Source: Author’s own elaboration

Interview guidelines

Table 51 – Overview of the interview guidelines for Phase 1

Section	Sub-section	N	Question	EU bodies	Academia & Think tanks
Introduction	Role	1	Please could you describe your role and how long you have been working / researching in the area of European law enforcement cooperation?	x	x
Threat landscape	Future challenges	2	In your view, what will be the main changes in the threat landscape in the next 5-10 years, and what tools will law enforcement authorities need to respond? <i>- What are the developments in the threat landscape?</i> <i>- How does the current legal framework help to respond to this?</i> <i>- In case changes are needed, then what kind of changes?</i>	x	x
The current EU Framework for law enforcement cooperation	Operational cooperation	3	Overall, to what extent is the current EU framework for operational cooperation effective in supporting cross border efforts to: - tackle serious organised crime? - ensure public order/safety across the EU? What works well? What are the main weaknesses and gaps?	x	x
The current EU Framework for law enforcement cooperation	Information sharing	4	Overall, to what extent is the current EU framework for information sharing (including legal and non-legal measures) effective in supporting cross border efforts to: - tackle serious organised crime? - ensure public order/safety across the EU? What works well? What are the main weaknesses and gaps?	x	x
The current EU Framework for law enforcement cooperation	Operational cooperation	5	Overall, do you consider the following Manuals, guidelines and catalogue clear, precise and complete enough to ensure the proper implementation of the Swedish Framework Decision, the Schengen acquis (CISA Convention), Prüm decisions on joint operations and other documents they refer to? <i>- Updated Catalogue of Recommendations for the correct application of the Schengen Acquis and Best practices: Police cooperation (15785/3/10);</i> <i>- Guidelines on the implementation of the SFD (13034/14);</i> <i>- Draft Guidelines for a Single Point of Contact (SPOC) for international law enforcement information exchange (10492/14);</i> <i>- Manual on cross border cooperation (13887/20);</i> <i>- Manual on Law Enforcement Information Exchange (5825/20)</i>	x	x
The current EU Framework for law enforcement cooperation	Structures for cooperation	6	There are a number of structures that exist to facilitate law enforcement cooperation (SPOCs; PCCCs, National SIRENE Bureaux; ENUs; Europol Liaison Officers; and/or others mentioned in the Manual on Law Enforcement Information Exchange National Fact Sheets; Manual on cross border cooperation (13887/20).	x	x

Section	Sub-section	N	Question	EU bodies	Academia & Think tanks
			How often are these different structures used in practice? - Which ones are used more frequently, and which ones very infrequently? - To what extent are they used to tackle SOC? - To what extent are they used to support cooperation in relation to public order/safety? (e.g. football matches, tourism, major cultural events, natural disasters, health crises)?		
The current EU Framework for law enforcement cooperation	Structures for cooperation	7	To what extent are these structures operating as intended/ effective in facilitating cross-border law enforcement cooperation? - In relation to SOC - In relation to cooperation around football matches, public order, tourism, major events etc?	x	x
The current EU Framework for law enforcement cooperation	Structures for cooperation	8	Thinking about these structures, what are the barriers or facilitators to their use/ effectiveness? - Could you comment on their use by customs agencies, as well as policing agencies?	x	x
The current EU Framework for law enforcement cooperation	Platforms for exchange of information	9	There are a number of platforms available to facilitate exchange of information between law enforcement authorities (SIENA; SIRENE channel (for supplementary information exchange); Schengen Information System (SIS); Europol Information System (EIS); Interpol exchange channels and databases How often are these different platforms used in practice? - Which ones are used more frequently, and which ones very infrequently? - To what extent are they used to tackle SOC? - To what extent are they used to support cooperation in relation to public order/safety (e.g. football matches, tourism, major cultural events, natural disasters, health crises, safeguarding public order and preventing offences)?	x	x
The current EU Framework for law enforcement cooperation	Platforms for exchange of information	10	To what extent are these platforms operating as intended/ effective to facilitate law enforcement cooperation? - In relation to SOC - In relation to cooperation around football matches, public order, tourism, major events etc?	x	x
The current EU Framework for law enforcement cooperation	Platforms for exchange of information	11	Thinking about these platforms, what are the barriers or facilitators to their use/ effectiveness? Could you comment on their use by customs agencies, as well as policing agencies?	x	x
The current EU Framework for	Platforms for exchange of information	12	Are there any other platforms or structures , not listed in the questions above, that are used to facilitate cooperation or the exchange of information which you consider particularly effective ?	x	x

Section	Sub-section	N	Question	EU bodies	Academia & Think tanks
law enforcement cooperation					
The current EU Framework for law enforcement cooperation	Platforms for exchange of information	13	There are some investigative tools - such as surveillance, interception of communications, covert investigations, controlled deliveries, using informants, undertaking hot pursuit, etc - that are considered essential to effectively tackle cross border SOC. Largely, however, these tools are defined and regulated by national law. What are the issues that arise, in practice, as a result of this lack of harmonisation?	x	x
The current EU Framework for law enforcement cooperation	Investigative tools for cross border crimes	14	What are the barriers or facilitators to the effective use of these tools in cross border investigations?	x	x
The current EU Framework for law enforcement cooperation	Investigative tools for cross border crimes	15	Which investigative tools would you prioritise for harmonisation at the EU level (if any)? Why?	x	x
Investigative tools used at the National level to combat organised crime		16	In this study we are aiming to identify investigative tools <i>available at the Member State level</i> (but not currently covered at all at the EU level) that are important to tackling serious organised crime. We are aiming to understand if there would be a benefit from minimum EU standards relating to these tools, in order to facilitate their use in cross-border investigations. In this context, are there any investigative tools used at the national level, not mentioned in your previous answers, that you think the study should be aware of?	x	x
Multilateral Agreements		17	There are number of bi/tri and multi-lateral agreements between Member States (for example, between the Nordic countries, DE-CH; DE-CZ...) which provide the basis for law enforcement cooperation. Are there any parts of these agreements that you consider to be particularly effective/ examples of good practice, and which might be incorporated into new EU measures to facilitate cross border cooperation? - Why? Why not? Can you elaborate about how they work in practice? -Please comment on whether they are used relation to investigations to tackle SOC, and/ or to support cooperation in relation to public order/safety?	x	x
Need for EU action and possible solutions	Need for EU Action	18	To what extent, in your view, is there a need for EU intervention to improve cross border law enforcement cooperation, investigation and information sharing in the fight and prevention of serious organised crime and/ or to ensure public order/safety?	x	x

Section	Sub-section	N	Question	EU bodies	Academia & Think tanks
Need for EU action and possible solutions	Policy Options	19	What policy solutions would you suggest improving: operational cooperation; information sharing; effective use of investigative tools?	x	x
Conclusion		20	Are there any other points you would like to add to inform the study?	x	x

Source: Author's own elaboration

Focus group guidelines

Reminder of the aim of the Focus groups with parties involved in bi/tri/multilateral agreements: to gather Member States' insights from an operational perspective on the practical implementation/use/effectiveness of bi/tri/multilateral agreements for cross-border law enforcement cooperation (including related measures/practices and investigative tools) in view of understanding to what extent these agreements extend beyond the current EU framework and of identifying possible good/best practices.

Each focus groups will last **around three hours** and will be structured in the following parts:

Introduction

- *Tour de table* – presentation of participants
- Aim of the study
- Purpose of the focus group
- Use of information collected (confidentiality, anonymity, use of restricted information)
- Permission to record

Part 1 Recent practical example of use

Aim: to hear about a recent use of the agreement to get a more detailed understanding of how they are used in practice and frame the discussion

Could you tell us about a recent example of cooperation using the agreement?

- What was the objective of the cooperation?
- Who was involved (which agencies)?
- What authorisations were needed to trigger the use of the agreement, if any?
- What happened and what was the result?
- What reporting etc. is needed, if any, after the agreement is used?
- What worked well in terms of using the agreement in this case?
- What were the areas for improvement?
- Would there have been a legal basis for this cooperation activity without the agreement? (would the cooperation have been possible without the agreement?)

Part 2 Scope: forms of cooperation

Aim: to understand all the forms of cooperation covered. This would be based on a prior, detailed analysis of the agreement, so we can prompt to understand the specific activities.

We understand that the agreement covers [*list - content based on in depth review of agreement*], could you help us understand the following [*list - clarification, for example, about:*

- *Operational activities (Joint patrols, Joint stations, etc)*
- *Equipment*
- *Training*
- *Investigative tools*

Part 3 Scope: information sharing

Aim: to understand what the agreement covers in terms of information sharing. This would be based on a prior, detailed analysis of the agreement, so we can prompt to understand the specific provisions.

We understand that the agreement covers [*list - content based on in depth review of agreement*], could you help us understand the following [*list - clarification, for example, about:*

- Access to databases
- Types of information shared
- Admissibility in court]

Part 4 Scope: Actors

Aim: to understand the actors covered. This would be based on a prior, detailed analysis of the agreement, so we can prompt to understand the specific actors.

We understand that the actors covered by the agreement are [policing agencies, customs, tax authorities, migration services etc].

- Could you tell us about how often these different actors are actually engaged in participation?
- What are the key barriers hindering participation by some agencies?
- Are there any actors not covered by the agreement who you think should be?

Part 5: Authorisations and oversight

Aim: to understand what steps have to be taken to use the powers in the agreement, and how these work in practice. This would be based on a prior, detailed analysis of the agreement, so we can prompt to understand the specific authorisations

- From our review, we understand that [xx] parts of the agreement need to be authorised by [Senior police officer/ prosecutor/ judge]. Could you tell us how this works in practice? (What evidence is needed to be presented, how long does it take etc.)?
- From our review, we understand that [xx] parts of the agreement need to be overseen by [Senior police officer/ prosecutor/ judge]. Could you tell us how this works in practice?

Part 6: Value added and complementarity

Aim: to understand what the agreement adds, compared to only relying on EU framework

- Without this agreement what would be the legal basis for the cooperation activities?
- What does the agreement add to the wider EU framework for cooperation and information exchange?

Part 7: Good practices and areas for improvement

- Which parts of the agreement are most effective? Why?
- Which parts of the agreement are least effective? Why?
- Do you think any parts of the agreement could be replicated at an EU-wide level to facilitate cooperation?
- Are there any other points you would like to add?

Case study interviews guidelines

Instructions

The topics should be addressed one by one (i.e. not first present all of the issues / POs), followed by questions:

- Short introduction to the first topic, i.e. info exchange;
- Questions and discussion with stakeholders (see questions, aspects to consider at the end of the doc);
- Second topic, i.e. joint operations;
- Third topic, i.e. investigative tools.

Potential Solutions

Table 52 – Guidelines for the case study interviews – Information Exchange

Topic / issue	Potential solutions
Legal barrier: Law enforcement authorities face difficulties in interpreting and implementing relevant EU provisions on access to and exchange of information. Moreover, the national rules on access to information impose procedural and administrative obstacles that prevent law enforcement authorities from other Member States from receiving such information in an effective and efficient way	• Clarification of the scope of the SFD: Clarification of the types of operations to which the SFD applies and definition of the competences LEAs need to have for its application • Establishment of a common minimum set of data that has to be made available for exchange and tightening the grounds for refusal in the SFD. The common minimum set could encompass e.g. the data that is available in at 10 Member States / SAC: ◦ Wanted/missing persons ◦ Persons suspected of criminal activities (criminal intelligence) ◦ Stolen goods ◦ Database of firearms ◦ Photographs (persons) ◦ Persons suspected of (a specific) crime ◦ Persons convicted of crime (criminal records) ◦ Passports and identity documents ◦ Border controls, border crossings and other border guard matters ◦ Reports (complaints) concerning crimes committed • New provisions ensuring compliance with deadlines by which data are to be made available to another Member State (including when a judicial authorisation is required). • Establishment of the information channel to be used: Establishment of SIENA as the preferred / default channel of communication for information exchange in an intra-EU context. Interpol i24/7 should be used in cases where third countries are involved in the exchange of information and if third countries do not concluded a cooperation agreement with Europol and do not have access to SIENA. SIENA would need to be monitored 24/7. There would also be an obligation to put Europol in copy when in cases within Europol's mandate.

Topic / issue	Potential solutions
	The following non-legislative improvements to SIENA would also be made: ○ Establishment of new, simpler and more user-friendly forms (e.g. design and accessibility, types of information required and clarifications and wording, multiple-choice alternatives, removal of references to “other cases”) and implementation of these in SIENA. The forms should include factual reasons for the information request. ○ Extension of the functionalities of SIENA, such as the introduction of (i) An automated display of a hit/not threshold (plus possibility to request further information) • Adaptations to the SFD to remove references to “other” cases and the forms for information exchange: Removal of the reference to “other” cases in the SFD and removal of the two annexes on information exchange. • Adaptations to the SFD to ensure alignment with the Law Enforcement Data Protection Directive, notably Article 8 on data protection. • Flanking non-legislative measures: Training, updated guidance (e.g. on SIENA), provision of a matrix concerning which information channel should be used in what cases, provision of information concerning what data are available in the MS (beyond the minimum required set). Internal Security Fund support for the SIENA roll-out.
Technical barrier: Law enforcement authorities have outdated IT infrastructure	• Establishment of common requirements for case management systems (CMS) for the SPOC: ○ Clearly define the CMS, including whether according to the national legislation (a) CMS is a database or (b) a workflow system (incl. establishment of data retention requirements in line with GDPR, Interpol, SIRENE, etc.) ○ Provide a list of common requirements for functionalities of the CMS, e.g.: ▪ Degrees of urgency should be linked with a deadline (e.g. when deadline draws near, alerts should be triggered) ▪ Selection (in a multiple-choice list by the requesting MS) and cancellation of the degrees of urgency should be done manually ▪ One CMS for receiving, sending and dispatching messages (follow up, manage, store and exploit the international exchange of information). Universal message format to be used ▪ CMS should be able to import and export incoming messages from e-mail, documents or web applications to reduce the number of registration acts to the minimum. The same is valid for exportation of generated messages ▪ Clear identification of the case and its components: Within the case (unique case number), all documents and acts should be clearly identified. The CMS should be able to make links about persons/objects; Per item – per act: author, date and time:

Topic / issue	Potential solutions
	this should be done automatically on the basis of the user profile. ▪ Automation of data cross-check, e.g. through improved search tools and the adoption of transliteration and “fuzzy logic” search ▪ Generation of proper statistics for national analytical needs and as required by EU law (e.g. SIS Regulation). ○ Accreditation of CMS (security needs, security check for data access, data protection, handling codes, confidentiality, access rights by different units and to EU databases) ○ Quality control: Through subject-based registration and the use of structured and mandatory fields and multiple-choice lists, certain quality requirements can be met beforehand without needing to conduct additional checks afterwards. ○ Availability of technical support • Secure communications: Non-legislative measure: Feasibility study on how to improve the secure digital and radio communication between the Member States. Support to the work of the EU innovation hub and of the RECG (Radio-communication Expert Group – Sub-group of the LEWP) • Flanking non-legislative measures: Training on CMS use, etc.
Structural barrier: National and regional information hubs set up by law enforcement authorities have different roles, means and capabilities, which make their cooperation sub-optimal. Law enforcement authorities have insufficient knowledge of existing mechanisms and skill gaps.	• Establishment of the SPOC as a “one stop shop” for LEA cooperation through common minimum standards. A SPOC should: ○ Be set up through its own national legislative or regulation identity ○ Be, at the minimum, informed about all international law enforcement cooperation requests dealt with at national level, and, in addition, be established as the preferred hub to handle intra-EU law enforcement cooperation requests ○ Operate 24/7 (including having a judicial authority available 24/7 “within” the SPOC) ○ Have full access to EU and international law enforcement databases (i.e. SIS, Europol databases, Interpol databases and software applications such as EUCARIS) ○ Be connected to SIENA (for intra-EU cases & Member States), i24/7 (for cases involving third countries), SIS, the SIRENemail network, and TESTA-NG. ○ Involve staff in the SPOC who have full access to all relevant national case management systems (including those managed by customs and border guards) ○ Ensure that all relevant information from the PCCCs is integrated in the SPOC information system ○ Have arrangements for indirect (e.g. on a hit/no hit basis), but quick, effective and efficient access to relevant databases of other authorities or bodies (including customs and border guards)

Topic / issue	Potential solutions
	○ Have full computerized access to hotel registers, should the need arise (the Article 45 CISA) ○ Ensure further coordination between the SPOCs and the PCCCs and other relevant entities such as the national EMPACT coordination and the network of EMPACT actors • Establishment of new provisions on the skills of law enforcement officials working primarily on international cases: ○ Provision on appropriate English skills as a criterion ("entry criterion") for specific roles within certain law enforcement agencies working primarily on international cases ○ Provision on mandatory training on EU law enforcement cooperation for officials in specific roles relevant for cross-border law enforcement and at specific levels (e.g. newcomers / senior officials) • Establishment of flanking soft measures in the form of training measures: ○ Establishment of an awareness raising and training campaign within the EU law enforcement community ○ CEPOL to provide training material to law enforcement agencies e.g. on how to use EU databases efficiently. The training material should focus on aspects common to all the Member States. The Member States would need to prepare additional training on the specificities in the individual country. ○ CEPOL to provide voluntary induction training on cross-border law enforcement ○ Expansion of the existing CEPOL practice to provide online courses on an ad-hoc basis on new EU level developments ○ Performance of a regular review of the training content provided by CEPOL

Source: Author's own elaboration

Table 53 – Guidelines for the case study interviews – Joint Operations

Topic / issue	Potential solution
Legal barrier: Law enforcement officials operating in other Member States often have inadequate powers to be able to provide efficient support. Moreover, these powers vary between the Member States,	• New provision on the conferral of powers: The host MS should confer certain operational powers to officials of seconding MS that are involved in joint operations. Exceptions may / may not be defined. See, for instance, Council Decision 2008/617/JHA Article 3.2 and 3.3: Subject to agreement between the Member States concerned, assistance may consist of providing the requesting Member State with equipment and/or expertise and/or of carrying out actions on the territory of that Member State, using weapons if so required. In the case of actions on the territory of the requesting Member State, officials of the assisting special intervention unit shall be authorised to operate in a supporting capacity on the territory of the requesting Member State and take all necessary measures to provide the requested assistance in so far as they (i) operate under the responsibility, authority and

Topic / issue	Potential solution
which leads to confusion	direction of the requesting Member State and in accordance with the law of the requesting Member State; and (ii) operate within the limits of their powers under their national law. • This should at minimum enable seconded officials to autonomously perform basic police tasks such as identity checks, vehicle and body search. This includes the running of identification data in relevant databases. • Flanking non-legislative measures: awareness raising and training, etc
Technical barrier: Officials on the ground are not able to efficiently access the information they need to ensure public order and safety.	• New provision on the remote access to relevant law enforcement databases in specific situations: The Member States are to provide [their own] officials on the ground remote access to specified police databases (or even specified data within them) in relation to specific types of international events (large-scale international football matches, mass tourism and music events, protection of VIPs etc.) via mobile terminals in specific geographical areas, such as major cities or regions where large-scale events take place more frequently. Restrictions on the use of specific types of information by the officials on the ground, including what information may be shared with officials from other countries, would be defined. • Flanking non-legislative measures, such as training
Structural barrier: National law enforcement authorities have limited financial and human resources to ensure an adequate use of joint operations.	• Establishment of an appropriate financial instrument by the Commission (e.g. through the ISF) to contribute to the funding of joint patrols in terms of staff costs; travel costs; accommodation; and expenses. • Flanking non-legislative measures
Structural barrier: Cooperation between law enforcement authorities in different countries, e.g. for the purpose of joint operations notably in border regions, is insufficiently informed by joint threat assessment/risk analysis.	• New provision on cross-border threat assessment: The Member States are to cooperate with neighbouring Member States to develop and use cross border threat assessment to better assess the need for joint operations and better inform their planning. • Flanking non-legislative measures: ○ Perform a pilot project to identify approaches to improve the development and use of joint threat assessment and risk analysis ○ Development of data collection tools (questionnaire and manual) specifically for customs

Source: Author's own elaboration

Table 54 – Guidelines for the case study interviews – Operational cooperation in relation to SOC and terrorism

Topic / issue	Potential solution
Legal driver: Law enforcement authorities are not able to efficiently use investigative tools in a cross-border context and face obstacles caused by differences in national rules.	• New provisions on surveillance: ○ Extend the current EU legal provisions to also cover the use of cross-border surveillance in relation to waterways, sea and air borders ○ Establish the possibility to start physical surveillance operations on the territory of another Member State ○ Simplify the legal requirements notably for a surveillance operation transiting by a Member State ○ Extend the list of offences in relation to which cross-border surveillance is allowed. In addition to the offences included in Articles 40-41 CISA, the extended list would cover the following offences: Extraditable offence (crimes for which the European Arrest Warrant is required); fleeing custody. ○ Streamline the definitions of "pre-planned" and "urgent" surveillance in the relevant legislative provisions on EU level ○ Ensure the possibility for technical means of surveillance (e.g. GPS tracker, drone) ○ Define a common maximum time allowed to carry out cross-border surveillance activities, e.g. specific time as smallest common denominator: 24 hours / 14 days ○ Accept and cooperate with the institutions responsible to oversee cross-border implementation of investigative tools in other Member States • New provisions on hot pursuit: ○ Extend the current EU legal provisions to also cover the use of cross-border hot pursuit in relation to waterways, sea and air borders ○ Extension of offences in relation to which cross-border hot pursuit is allowed. In addition to the offences included in Articles 40-41 CISA, the extended list could cover the following offences: Extraditable offence (crimes under the European Arrest Warrant); fleeing custody; ○ Permit cross-border hot pursuit continue for at least an hour ○ Establish common rules for hot pursuit, e.g.: (i) Permit the requesting party the right to continue the hot pursuit if the requested party cannot take over the pursuit in time at a minimum; (ii) Permit hot pursuit beyond extraditable offences if someone avoids police or border checks without any time and territorial restrictions; Permit hot pursuit without any distance limit ○ Establish minimum standards on the rights and duties of the pursuing officials, including the right to: search a person; put on handcuffs; apprehend; detain; stop cars; perform preliminary arrest, if local authorities do not arrive on time ○ Flanking non-legislative measures, such training and joint operation simulation exercises • Controlled delivery: Common minimum approximation of national rules to facilitate its use in a cross-border context

Topic / issue	Potential solution
	• Interception of communication: Common minimum approximation of national rules to facilitate its use in a cross-border context

Source: Author's own elaboration

Questions in relation to the potential solutions

Instructions: The following are high-level questions to guide the conversations with the stakeholders. Based on the feedback provided by the stakeholders, follow-up questions should be raised.

- To what extent can you confirm that the identified issues are relevant problems you face in your daily work?
- To what extent do you think the potential solutions identified could:
 - a) Facilitate your daily routine / the work on the ground?
 - b) Improve cross-border cooperation in relation to public order and safety, as well as serious and organised crime?
- Would any of the solutions identified have adverse effects, i.e. negative impacts for specific groups of stakeholders or in certain cases etc.? Could any other solution be implemented instead to address the problems?
- Do you have any practical examples to illustrate your views? Do you have specific analyses, quantitative data etc. at hand that we could be used to substantiate the arguments?

The following table serves as an overview of the potential impacts the policy options can have. Based on the discussion with the stakeholders, please choose relevant aspects to focus on.

Table 55 – Overview of potential impacts of the policy options

Operational dimension	Policy and societal dimension
<u>Qualitative:</u> Access to information: • Technical access and better usability (e.g. of forms and systems such as SIENA) • Streamlined awareness and knowledge across officers • Improved search results in databases • Reduced working time to provide, share, and analyse information Quality and efficiency of operational cooperation: • Reduced working time due to better information to act on (solving cases instead of managing them) • Reduced waiting time / time delays (e.g. due to waiting for information from LEAs in other countries) • Progress towards “seamless job experience” (i.e. no difference between cross-border and domestic cases) Improved awareness, knowledge, and skills: • Understanding of officers’ competencies and duties in cross-border operations • Competencies and preparedness of officers for cross-border operations • Improved ability of officers to focus on cross-border operations (“becoming an expert”)	<u>Qualitative:</u> Clarity of the regulatory framework: • Accessibility of applicable legislation • Awareness and knowledge of SPOCs / PCCCs about the operations of their counterparts in other MS Coherence of technical aspects of cross-border cooperation: • MS’ technical abilities in terms of accessing and sharing information increasingly satisfy “common minimum standards” Coherence concerning the operational set-up and coordination: • MS’ organisational set-up satisfies “common minimum standards” • MS increasingly learn from each other • MS are increasingly active in engaging with Europol Less risks related to SOC and situations critical for public order, e.g. due to: • Increased use of information exchange, joint operations and investigative tools • Risk analyses being co-developed by and shared between MS and with Europol • Broad use of common standards for risk analysis
<u>Quantitative:</u> Effective cross-border law enforcement cooperation more frequently in terms of: • Information requests exchanged between MS, as well as MS and Europol • Joint operations • Use of investigative tools Increased effectiveness of cross-border law enforcement cooperation: • More cross-border cases can be prevented / solved • More complex and important cross-border cases can be prevented / solved Increased efficiency of cross-border law enforcement cooperation: • Fewer delays in cross-border operations • Less time needed for case management • Fewer resources needed for case management, i.e. more resources spent on „solving cases“ • Increased budgetary spending on cross-border operations, e.g. Staff; Travel; Accommodation; Expenses. • Increased budgetary spending on officers’ training	

Source: Author’s own elaboration

5.2 List of stakeholders consulted

Interviews

EU Bodies

Table 56 – Overview of the number of stakeholders consulted from EU bodies

EU Body/Institutions	N° of Interviewees	
	Phase 1	Phase 2
CEPOL	1	2
EDPS	1	1
EJN	1	1
EJTN	2	0
EMCDDA	1	0
EPPO	1	1
EUCPN/ENAA	1	2
Eurojust	1	0
Europol	1	4
FRA	1	1
OLAF	1	1

Source: Author's own elaboration

Academia and Think Tanks

Table 57 – Overview of the number of stakeholders consulted from academia and think tanks

Institution	N° of Interviewees
Leiden University	1
Queen Mary University of London	1
Tilburg University	1
Transcrime (Università Cattolica of Milan)	1

Source: Author's own elaboration

EMPACT Drivers

Table 58 – Overview of the number of stakeholders consulted from EMPACT Drivers

Member State	Priority	N° of Interviewees
Belgium	Cybercrime	1
France	Horizontal Expert Group on Document fraud	1
France	Environmental Crime	1
France	Organised Property Crime	1
Greece	Facilitating Illegal immigration	1
Italy	MTIC fraud	1
Lithuania	Excise Fraud	1
Spain	Firearms	1
Spain	Drugs	1
Germany	Member of International police cooperation of the criminal police	1

Source: Author's own elaboration

EMPACT Support Managers

Table 59 – Overview of the number of stakeholders consulted from EMPACT Support Managers

Priority	N° of Interviewees
Money laundering	1
Cybercrime - CSA/CSE	2
Excise and MTIC fraud	3
Environmental crime	1
OPC	1
Cybercrime – Cyber attacks on information system	1
Cybercrime – Non-cash payment Fraud	1
Criminal Finances, Money Laundering and Asset Recovery	1

Source: Author's own elaboration

Online survey

LEAs

Table 60 – Overview of the stakeholders consulted from LEAs

Country	Institution (n° of respondents)
Austria	Bundesministerium für Inneres
	Criminal intelligence service
	Ministry of Finance - Tax and Customs Administration
Belgium	Belgian federal police
	General Administration of Customs and Excises
Bulgaria	National Customs Agency of the Republic of Bulgaria
	Ministry of Interior
Croatia	Customs
	General Police Directorate, Criminal Police Directorate, General Crime Service (OPC and envir. Crime)
Cyprus	Cyprus police - c.i.d. (ops)
	Department of Customs and Excise
	Intelligence management analysis subdirectorates
	N.f.i.p. cyprus police
Czech Republic	Customs
	The Police Presidium of the Czech Republic; Division for International Police Cooperation
	Police of the Czech Republic, National Organised Crime Agency
	Ministry of Interior
Denmark	Special investigation west / east jutland police
	Danish national police
	Copenhagen police - border crime centre oeresund
	Pccc padborg
	National Centre of Investigation
Estonia	Sydsjællands og Lolland Falsters politi
	Estonian Police and Border Guard Board
Finland	National Bureau of Investigation / Finnish Police
	National police board
	Finnish border guard
	Nbi finland /spoc
	Finnish Police / National Bureau of Investigation
France	Finnish customs
	Antinarcotics agency (ofast)
	Border police central directorate
	DCI - Direction de la coopération internationale
	Dgddi
	French national border directorate
	Gendarmerie nationale
	National football information point

Country	Institution (n° of respondents)
	National Gendarmerie / Central Service for Criminal Intelligence
	OCLDI - Central Office fighting against mobile organised crime
	Oclti
	Sirasco
	Bmi
Germany	Bundeskriminalamt/federal criminal police office
	Central customs authority
Greece	Hellenic police
	International law enforcement cooperation centre
	National Bureau of Investigation
Hungary	DG Law Enforcement Public Safety Protection and Guard
	Dg law enforcement duty department
	National Tax and Customs Administration
Ireland	An garda siochana - irish police
Latvia	State Revenue Service, Tax and Customs Police Department
Liechtenstein	Pccc schaanwald
	National police
Lithuania	Police Department under moi Public Police Board Response and Readiness Unit NFIP Lithuania
	Customs criminal service
Luxembourg	Grand ducal police
Malta	Customs
Netherlands	Customs
	Ministry of Justice and Security
Norway	National police directorate
Poland	Ministry of Finance / National Revenue Administration
	Polícia de Segurança Pública
	Polícia judiciária
Portugal	Internal security system
	Guardia nacional republicana
	Tax and Customs Authority
	Polícia judiciária - ct national unit (unct)
Romania	General Directorate for Operational Management - Ministry of Internal Affairs - Romania
	National Football Information Point - General Inspectorate of the Romanian Gendarmerie
	Ministry of Interior of the Slovak Republic
Slovakia	National crime agency (naka)
	Presidium of Police Force, Criminal Police Bureau, Spectator Violence Unit, National Football Information Point
	Presidium of the Police Corps, Criminal Police Office, Department of Criminal Investigation
Slovenia	General police directorate
	Policia nacional
	Nfip - policia nacional
Spain	State Secretary for Security
	Comisaría General de Policia Judicial- Unidad Central de Delincuencia Especializada y Violenta- Brigada de Patrimonio Histórico
	Customs
Sweden	Customs
	The swedish police authority
Switzerland	Swiss Federal Office of Police fedpol

Source: Author's own elaboration

National Judicial Authorities

Table 61 – Overview of the stakeholders consulted from National Judicial Authorities

Country	Institution (n° of respondents)
Cyprus	Eurojust National Member
Estonia	Eurojust National Member
Germany	Eurojust National Member
Latvia	Eurojust National Member
Netherlands	Eurojust National Member
Norway	Eurojust National Member
Portugal	Eurojust National Member
Romania	Eurojust National Member
Slovakia	Eurojust National Member
Sweden	Eurojust National Member
Switzerland	Eurojust National Member

Source: Author's own elaboration

National Data Protection Authorities

Table 62 – Overview of the stakeholders consulted from National Data Protection Authorities

Country	Institution (n° of respondents)
Belgium	National Data Protection Authority
Bulgaria	National Data Protection Authority
Croatia	National Data Protection Authority
Cyprus	National Data Protection Authority
Estonia	National Data Protection Authority
Hungary	National Data Protection Authority
Lithuania	National Data Protection Authority
Poland	National Data Protection Authority
Romania	National Data Protection Authority
Slovenia	National Data Protection Authority

Source: Author's own elaboration

Focus groups

Benelux Agreement

Table 63 – Overview of the stakeholders consulted with respect to the Benelux Agreement

Country	Institution (n° of participants)
Belgium	Federal Police (2)
Luxembourg	Police Grand-Ducale (2)
Netherlands	Netherlands Defence Academy
Netherlands	Ministry of Justice and Security (2)
Netherlands	National Police (2)

Source: Author's own elaboration

Czechia-Germany Agreement

Table 64 – Overview of the stakeholders consulted with respect to the Czechia-Germany Agreement

Country	Institution (n° of participants)
Czechia	International police cooperation directorate (3)
Czechia	Czech republic liaison officer
Germany	Police Academy Hamburg
Germany	Customs
Germany	Bavarian State Police
Germany	PCCC
Germany	Ministry of Finance (2)

Source: Author's own elaboration

France-Switzerland Agreement

Table 65 – Overview of the stakeholders consulted with respect to the France-Switzerland Agreement

Country	Institution (n° of participants)
France	Secrétariat général des affaires européennes
France	Direction de la Coopération Internationale (DCI) (2)
France	Service de la Justice et des affaires intérieures (2)
France	Police Nationale
France	Gendarmerie
Switzerland	Federal Police
Switzerland	Département de la sécurité, de l'emploi et de la santé (3)

Source: Author's own elaboration

Nordic Agreement

Table 66 – Overview of the stakeholders consulted with respect to the Nordic Agreement

Country	Institution (n° of participants)
Denmark	National Police (3)
Finland	National Police (3)
Iceland	National Police (3)
Norway	National Police (2)
Sweden	Swedish Police Authority (4)
Sweden	Customs

Source: Author's own elaboration

Case study interviews

Table 67 – Overview of the stakeholders consulted as part of case studies

Country	Institution (n° of case study interviews)
Austria	Ministry of the Interior (1)
France	Ministry of the Interior, National Police, Gendarmerie (4)
Slovenia	Ministry of the Interior, Criminal Police Directorate (4)
Sweden	National Police (1)
Switzerland	Federal Police (2)

Source: Author's own elaboration

6 BIBLIOGRAPHY AND MAIN SOURCES OF INFORMATION

EU Legal framework

Convention on close cooperation between EU customs administrations (**Naples II Convention**) (1998).

Consolidated version of the **Treaty of the Functioning of the European Union** (2008).

Council Decision 2006/560/JHA of 24 July 2006 amending Decision 2003/170/JHA on the common use of liaison officers posted abroad by the law enforcement agencies of the Member States.

Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union (2006).

Council Decision 2007/412/JHA of 12 June 2007 amending Decision 2002/348/JHA concerning security in connection with football matches with an international dimension.

Council Decision 2008/615/JHA of 23 June 2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime (2008).

Prüm Convention on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration 2005.

The **Schengen acquis** - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders (1990).

Information sharing

Communication from the Commission to The European Parliament and the Council Implementing the European Agenda on Security: **EU action plan against illicit trafficking in and use of firearms and explosives (COM/2015/624 final)**.

Council Decision of 25 April 2002 concerning security in connection with football matches with an international dimension (**2002/348/JHA**).

Council Decision 2005/671/JHA of 20 September 2005 on the exchange of information and cooperation concerning terrorist offences.

Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences.

Council Decision 2009/917/JHA of 30 November 2009 on the use of information technology for customs purposes.

Council Document 14755/1/12, 15 November 2012.

Council Document 14623/17, 27 November 2017. (LIMITE).

Council Document 14629/17, 27 November 2017. (LIMITE).

Council Document 6552/19, 11 March 2019. (LIMITE).

Council Document 12093/19, 7 October 2019.

Council Document, 5825/20, 2 December 2020. (LIMITE).

Council Document 5503/21, 28 January 2021. (LIMITE).

Council Document 5517/21, 28 January 2021.(LIMITE).

Council Document 6257/21, 25 March 2021. (LIMITE).

Council Framework Decision 2002/475/JHA of 13 June 2002.

Council Regulation (EC) No 515/97 of 13 March 1997 on mutual assistance between the administrative authorities of the Member States and cooperation between the latter and the Commission to ensure the correct application of the law on customs and agricultural matters.

Framework Decision 2002/584/JHA.

Council Resolution of 4 December 2006 concerning an updated **handbook with recommendations for international police cooperation** and measures to prevent and control violence and disturbances in connection with football matches with an international dimension, in which at least one Member State is involved (2006/C 322/01- Football Handbook).

Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime. Member States were required to incorporate the directive into national law by 25 May 2018.

Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011, applicable since 11 December 2018.

Regulation (EU) 2018/1860 of the European Parliament and of the Council of 28 November 2018 on the use of the Schengen Information System for the return of illegally staying third-country nationals.

Regulation (EU) 2018/1861 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks, and amending the Convention implementing the Schengen Agreement, and amending and repealing Regulation (EC) No 1987/2006.

Regulation (EU) 2018/1862 of the European Parliament and of the Council of 28 November 2018 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters, amending and repealing Council Decision 2007/533/JHA, and repealing Regulation (EC) No 1986/2006 of the European Parliament and of the Council and Commission Decision 2010/261/EU, applicable from 28 December 2021 at the latest.

Regulation (EU) 2019/818 of the European Parliament and of the Council of 20 May 2019 on establishing a framework for interoperability between EU information systems in the field of police and judicial cooperation, asylum and migration and amending Regulations (EU) 2018/1726, (EU) 2018/1862 and (EU) 2019/816.

Data protection

Charter of Fundamental Rights of the European Union.

Communication From The Commission To The European Parliament And The Council -Way forward on aligning the former third pillar acquis with data protection rules **COM/2020/262 final**.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - **COM/2017/010 final - 2017/03 (COD)**

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 with regard to the processing of personal data by the Union institutions, bodies, offices and agencies.

Council document 6087/21

EU Agencies

Council Act of 26 July 1995 drawing up the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (**Europol Convention**)

Commission Decision of 28 April 1999 establishing the European Anti-fraud Office (OLAF) (notified under document number SEC(1999) 802) (1999/352/EC, ECSC, Euratom).

Council Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime

Council Decision 2005/681/JHA establishing the European Police College (CEPOL) and repealing Decision.

Council Regulation (EC) No 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union.

Council Regulation (EEC) No 302/93 on the establishment of a European Monitoring Centre for Drugs and Drug Addiction.

Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

Regulation (EC) No 1920/2006 on the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA).

Regulations Council Regulation (EC) No 168/2007 of 15 February 2007 establishing a European Union Agency for Fundamental Rights.

Regulation (EU) 2015/2219 of the European Parliament and of the Council of 25 November 2015 on the European Union Agency for Law Enforcement Training (CEPOL) and replacing and repealing Council Decision 2005/681/JHA, applicable since 1 July 2016.

Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, applicable since 1 May 2017.

Council Regulation (EU) 2017/1939 of 12 October 2017 implementing enhanced cooperation on the establishment of the European Public Prosecutor's Office (EPPO).

Regulation (EU) 2018/1726 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA).

Regulation (EU) 2018/1727 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for Criminal Justice Cooperation (Eurojust), and replacing and repealing Council Decision 2002/187/JHA.

Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard (FRONTEX) and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624.

Additional sources related to police cooperation

Commission Recommendation (EU) 2017/820 of 12 May 2017 on proportionate police checks and police cooperation in the Schengen area (2017).

Commission Staff Working Document accompanying the document Report from the Commission to the Council and the European Parliament on the Functioning of the Schengen Evaluation and Monitoring Mechanism pursuant to Article 22 of Council Regulation (EU) No 1053/2013 First Multiannual Evaluation Programme (2015-2019) **SWD/2020/327** final.

Communication from the Commission to the European Parliament and the Council. A strategy towards a fully functioning and resilient Schengen area, **COM(2012) 277** final.

Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU security union strategy - **COM/2020/605** final (2020).

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy to tackle organised Crime 2021-2025, **SWD(2021) 74** final.

Council Decision 2008/616/JHA of 23 June 2008 on the implementation of Decision 2008/615/JHA on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime.

Council Decision 2008/617/JHA of 23 June 2008 on the improvement of cooperation between the special intervention units of the Member States of the European Union in crisis situations (2008).

Council of the European Union (2020) *Manual on Cross-border Cooperation*.

Council Document 10000/07, 25 May 2007.

Council Document 9512/10, 26 May 2010

Council Document 10505/4/09, 14 December 2009.

Council Document 15785/3/10, 15 March 2011.

Council Document 9105/11, 15 April 2011.

Council Document 6721/3/14, 3 June 2014.

Council Document 10492/14, 13 June 2014.

Council Document 13034/14, 17 September 2014.

Council Document 10597/15, 14 September 2015.

Council Document 15429/16, 21 December 2016. (LIMITE).

Council Document 6261/17, 4 July 2017.

Council Document 8586/18, 15 May 2018. (Not publicly available).

Council Document 10095/1/18, 25 September 2018. (LIMITE).

Council Document 6727/18, 25 October 2018.

Council Document 10062/19, 6 June 2019.

Council Document 10590/18, 4 July 2018. (LIMITE).

Council Document 10313/20, 4 September 2020. (LIMITE).

Council Document 11516/20, 12 October 2020. (LIMITE).

Council Document 13083/1/20, 24 November 2020.

Council Document 5825/20, 2 December 2020.

Council Document 13920/20, 15 December 2020. (LIMITE).

Council Document 10131/20. (LIMITE).

Council Document 13887/20, 16 December 2020.

Council Document 5517/21, 28 January 2021. (LIMITE).

Council Document 5449/21, 8 February 2021. (LIMITE).

Council Document 6256/21, 20 February 2021. (LIMITE).

Council document 7290/21, 23 March 2021. (LIMITE).

Council Document 7232/21, 24 March 2021. (LIMITE).

Council document 7233/21, 25 March 2021.(LIMITE).

Council Document 8014/1/21, 26 April 2021 (LIMITE).

Council of the European Union (2002), **EU Schengen Catalogue**: External borders control, Removal and readmission – recommendations and best practices.

Council of the European Union (2020) Enhancing cross-border law enforcement cooperation: Best practices, current challenges and way forward. Brussels: Council of the European Union.

Council of the European Union. (2021). The impact of the COVID-19 pandemic on internal security: threats, trends, resilience and lessons learned for Law Enforcement Agencies: outcomes of previous discussion and draft Council Conclusions. Brussels: Council of the European Union.

EU Convention on mutual assistance in criminal matters between Member States

Report from The Commission to The Council And The European Parliament on the Functioning of the Schengen Evaluation and Monitoring Mechanism pursuant to Article 22 of Council Regulation (EU) No 1053/2013 First Multiannual Evaluation Programme (2015-2019) **COM/2020/779 final**.

UN (1982) **Convention on the Law of the Sea**.

UN (2004) **Convention against Transnational Organised Crime**.

UN (2004) **Convention against Corruption**.

Bi/Tri/Multilateral agreements

AT-CH-LI - Agreement between the Principality of Liechtenstein, the Swiss Confederation and the Republic of Austria on Cross-Border Police Cooperation .

AT-CZ - Agreement between the Czech Republic and the Republic of Austria on police cooperation and on the second amendment to the European Convention on Mutual Assistance in Criminal Matters.

AT-DE - Contract between the Federal Republic of Germany and the Republic of Austria on cross-border cooperation in police-related deterrence of threats and criminal matters.

AT-HU - Agreement between the Republic of Austria and of the Republic of Hungary on cooperation for the prevention and investigation of cross-border crimes.

AT-IT - Agreement between the Government of the Republic of Austria and the Government of the Italian Republic on Police Cooperation.

AT-SI - Agreement between the Republic of Austria; and the Republic of Slovenia on police cooperation. Chapter II: General Forms of Police Cooperation.

AT-SK - Agreement between the Republic of Austria and the Slovak Republic on Police Cooperation.

Baltic Agreement (EE, LT, LV) - Agreement Between the Government of the Republic of Latvia, the Government of the Republic of Estonia and the Government of the Republic of Lithuania on Co-operation in Protection of Witnesses and Victims.

BE-DE - Agreement between the government of the Kingdom of Belgium and the government of the Bundesrepublik Germany on the cooperation of police and customs authorities in border areas, signed in Brussels on the 27th of March 2000.

BE-DE-FR-LU - Agreement between the Government of the Kingdom of Belgium, the Government of the Federal Republic of Germany, the Government of the French Republic and the Government of the Grand Duchy of Luxembourg, concerning the creation and operation of a common police and customs cooperation centre in the border.

BE-FR - Act agreeing to the Agreement between the Government of the Kingdom of Belgium and the Government of the French Republic on cross-border cooperation in police and customs matters, made in Tournai on 18 March 2013.

Benelux agreement (BE, NL, LU) - Treaty between the Kingdom of the Netherlands, Kingdom of Belgium and the Grand Duchy of Luxembourg on police cooperation.

BG-CH - Agreement between the Swiss Confederation and the government of the Republic of Bulgaria on cooperation to fight crimes.

BG-EL - Agreement between the Government of the Hellenic Republic and the Government for the Republic of Bulgaria on contact centre for cooperation.

BG-EL-RO - Protocol for the enhanced trilateral cooperation in combatting crime and especially trans-border crimes.

CH-CZ - Contract between the Swiss Confederation and the Czech Republic on police cooperation and the combatting of crimes.

CH-DE - Contract between the Swiss Confederation and the Federal Republic of Germany about the cross-Border Police and Judicial Cooperation.

CH-FR - Agreement between the Swiss Confederation and the government of the Republic of France on Cross-border Cooperation in judicial, police and custom matters.

CH-FR - Agreement between the Swiss Federal Council and the Principality of Liechtenstein for Cooperation in the Framework of Swiss Information Systems on Fingerprints and DNA Profiles ("the Agreement").

CH-HU - Agreement between the Swiss Confederation and the Republic of Hungary on the cooperation to combat crimes.

CH-IT - Agreement between the Swiss Confederation and the government of the Italian Republic on the cooperation of police and customs bodies.

CH-LV - Agreement between the Swiss Confederation and the Republic of Latvia on police cooperation to fight crimes.

CH-RO - Agreement between the Swiss Confederation and Romania on the cooperation in the fight of terrorism, organised crime, the illegal trade with drugs and other transnational crimes

CH-SI - Agreement between the Swiss Confederation and the Republic of Slovenia on the cooperation to fight crimes.

CY-ES - Agreement between the Republic of Cyprus and the Kingdom of Spain on cooperation in combatting organised crime.

CY-IE - Agreement between the Government of Ireland and the Government of the Republic of Cyprus on Co-operation in Combating Illicit Drug Trafficking, Money Laundering, Organised Crime, Trafficking in Persons, Terrorism and Other Serious Crime.

CY-IT - Agreement between the Government of the Republic of Cyprus and the government of the Republic of Italy on the cooperation in the fight against organised crime and other forms of crime.

CY-SK - Agreement between the Government of the Republic of Cyprus and the Government of the Slovak Republic on Co-operation in combating organised crime, terrorism, illicit trafficking in narcotic drugs and psychotropic substances as well as other types of crime.

CZ-DE - Contract between the Federal Republic of Germany and Czechia on police cooperation and the amendments to the contract from the 2. February 2000 between the Federal Republic of Germany and Czechia on the complement to the European Agreement for cooperation in criminal matters from the 20. April 1959 and its implementation.

CZ-PL - Treaty between the Czech Republic and the Republic of Poland on Cooperation in the Fight Against Crime, Protecting Public Order and Cooperation in Border Areas.

DE-DK - Agreement between the government of the Federal Republic of Germany and the government of the kingdom of Denmark on police cooperation in the border regions.

DE-FR - Agreement between the government of the Federal Republic of Germany and the French Republic on police and customs cooperation in the border regions.

DE-LU - Agreement between the Federal Minister of the Interior of the Federal Republic of Germany and the Minister of Justice and the Minister of Public order of the Grand Duchy of Luxembourg on police cooperation in the border area between the Federal Republic of Germany and the Grand Duchy of Luxembourg.

DE-NL - Treaty between the Bundesrepublik Germany and the Kingdom of the Netherlands on cross-border police cooperation and cooperation on law enforcement.

DE-PL - Agreement between the government of the Federal Republic of Germany and the government of the republic of Poland on police, border and customs cooperation.

EE-LV - Agreement between the government of the republic of Latvia and the Government of the Republic of Estonia on cross - border cooperation in combating crime, (2006).

EL-FR - Agreement between government the Hellenic Republic and the Government of the Republic of France cooperation in matters of internal security.

EL-HR - Agreement between government the Hellenic Republic and the Government of the Republic of Croatia on fighting against international illicit trafficking on narcotic drugs and psychotropic substances, international terrorism and organised crime.

EL-IT - Agreement on cross border police cooperation between the Republic of Italy and the Hellenic Republic

EL-MT - Agreement between the Government of the Hellenic Republic and the Government of Malta on cooperation between the Ministry of Public Order of the Hellenic Republic and the Ministry of Home Affairs of Malta on matters of their competence.

EL-PL - Agreement between government the Hellenic Republic and the Government of the Republic of Poland concerning the cooperation between the Hellenic Ministry of Public Order of the Hellenic Republic and the Ministry of the Interior of the Republic of Poland on matters of their competence.

EL-RO - Agreement between government of Romania and the government of the Hellenic Republic, concerning cooperation between the Ministry of Interior of Romania and the Ministry of Public Order of the Hellenic Republic, on matters of their competence.

EL-SI - Agreement between government of the government of the Hellenic Republic and the Republic of Slovenia on Cooperation in fighting crime, especially terrorism, illicit drug trafficking and organised crime.

ES-FR - Agreement on police and customs Cross-Border Cooperation between the Kingdom of Spain and the French Republic

ES-PT - Protocol between the Kingdom of Spain and the Portuguese Republic on Technical Cooperation and Mutual Assistance on Civil Protection

HR-SI - Agreement between the government of the Republic of Slovenia and the government of the Republic of Croatia on cross-border police cooperation.

HU-SI - Agreement between the Republic of Hungary and the Republic of Slovenia on cross-border co-operation of law enforcement authorities.

HU-SK - Agreement between the Slovak Republic and the Hungarian Republic on cooperation to prevent cross-border crime and fight against organised crime.

IT-SI - Agreement between the Government of the Republic of Slovenia and the Government of the Italian Republic on Cross - Border Police Cooperation.

LT-LV - Agreement on Cross Border Cooperation between the Police Department under the Ministry of the Interior of the Republic of Lithuania and the State Police of the Ministry of the Interior of the Republic of Latvia.

LT-PL - Agreement between the Government of the Republic of Poland and the Government of the Republic of Lithuania on cooperation in combating organized crime and other crimes and cooperation in border areas, signed in Vilnius on March 14, 2006. **Nordic Countries (DK, FI, IS, NO, SE)** - Nordic Administrative Agreement on Cooperation between Police Authorities in the Nordic countries.

PL-SK - Agreement between the Republic of Poland and the Slovak Republic, amending the Agreement between the Republic of Poland and the Slovak Republic on cooperation in combating crime and on cooperation.

Southeast Europe (AT, AL, BIH, BG, HR, HU, MD, MNE, NMK, RO, SRB, SI) - Police Cooperation Convention for Southeast Europe.

Reports, studies, academic literature and other documentation

BBC (2021), Suez Canal reopens after giant stranded ship is freed.

BBC News (2015) Paris attacks: What happened on the night.

BBC News (2016) Euro 2016: Who is to blame for the Marseille violence.

BBC News (2021) Swindon railway station as gateway for drug trafficking.

Bouvet-Gerbettaz, V. (2014). New in Europe: the first Franco-Swiss mixed operational brigade (BOM) is born. Academic and grey literature on police cooperation.

De Sousa, L. (2013) Understanding European Cross-border Cooperation: A Framework for Analysis, *Journal of European Integration*, 35:6, 669-687, DOI.

Der Tagesspiegel (2016) So funktioniert das Netz der Taschendiebe.

Deutsche Welle (2017) After G20: A look at left-wing radicalism in Europe.

Deutsche Welle (2021) COVID aid: Germany uncovers over 25,000 cases of fraud.

Di Nicola, A., Gounev, P., Levi, M., Rubin, J., Vettori, B., Baratto, G., Betgens, M., Bezlov, T., Bressan, S., Constantino, F., Cauduro, A. (2015), Study on paving the way for future policy initiatives in the field of fight against organised crime: the effectiveness of specific criminal law measures targeting organised crime.

Dupont, C., Verbari, M., Spanikova, H. (2016) Assessing the completeness and conformity of Member States measures to transpose Council Framework Decision 2006/960/JHA. Brussels: Milieu Ltd. (Unpublished).

EMCDDA (2021) European Drug Report 2021. Trends and Developments.

Euractiv (2020) EU signs €100m drone contract with Airbus and Israeli arms firms.

Eurofund (2020) Living, working and COVID-19, COVID-19 series, Publication Office of the European Union.

European Commission (2017) Boosting Growth and cohesion in EU border regions. Brussels: European Commission.

European Commission. (2018) Second report on the progress made in the fight against trafficking in human beings (2018) as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims.

European Commission. (2020) Report from the Commission to the European Parliament. Third report on the progress made in the fight against trafficking in human beings (2020) as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims {SWD (2020) 226 final}.

European Commission (2020) Report from the Commission to the Council and the European Parliament on the Functioning of the Schengen Evaluation and Monitoring Mechanisms pursuant to Article 22 of Council Regulation (EU) No 1053/2013 – First Multiannual Evaluation Programme (2015-2019). Brussels: European Commission.

European Commission (2020) Data collection on trafficking human beings in the EU.

European Commission (2020) A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond.

European Commission (2020) Use of Internet and Online Activities.

European Commission (2020) EU Security Union Strategy.

European Commission (2020) A EU Strategy to tackle Organised Crime 2021-2025.

European Commission. 2020. *Erasmus+ Annual Report 2019*. Luxembourg: Publications Office of the European Union.

European Commission (2021) Trafficking in firearms.

European Commission (2021) Communication from the Commission to the European Parliament and the Council - A strategy towards a fully functioning and resilient Schengen area. COM(2021) 277 final, 2 June, Brussels.

European Confederation of Police (EuroCOP) supporting Commission's initiative to streamline and consolidate existing instruments for cross-border police cooperation (November 2020). (Not publicly available).

European Parliament (2020) Organised Property Crime in the EU.

Europol (2017) Serious and Organised Crime Threat Assessment (SOCTA): Crime in the age of technology, European Union.

Europol (2015) Exploring Tomorrow's Organised Crime. The Hague: Europol.

- Europol (2019) Internet Organised Crime Threat Assessment (IOCTA).
- Europol (2020) Internet Organised Crime Threat Assessment (IOCTA) 2020. The Hague: Europol.
- Europol (2020) EU Terrorism Situation and Trend Report (TE-SAT) 2020. The Hague: Europol.
- Europol (2020) How COVID-19-related crime infected Europe during 2020. The Hague: Europol.
- Europol (2020) EU Policy Cycle – EMPACT.
- Europol (2020) COVID-19 Waste crime: Europe-wide operation to tackle unlawful sanitary waste disposal.
- Europol (2020) Cocaine Cartel shipping from South America busted in Spain and the Netherlands.
- Europol (2020) Customs thwart illegal cigarette trade in the EU and UK: 17 arrests and 67 million cigarettes seized.
- Europol (2021) Serious and Organised Crime Threat Assessment (SOCTA): A corrupting influence, European Union.
- Eurostat (2020) *People on the move – statistics on mobility in Europe*.
- Eurostat (2020) *EU citizens living in another Member State - statistical overview*.
- Eurostat (2020) *Which EU Countries had the highest GDP in 2019?*
- Eurostat (2021) Nights spent at tourist accommodation establishments by residents/non-residents.
- Eurostat (2021) Extra-EU imports of main CPA groups, 2015-2019.
- Eurostat (2021) Gross domestic product at market prices.
- EY, RAND (2020) Evaluation Study on the EU Policy Cycle for organised and serious international crime/EMPACT 2018-2021. (Unpublished).
- Fondazione Giacomo Brodolini (2018) Pilot Project on the Fundamental Rights Review of EU Data Collection instruments and Programmes.
- Frontex (2020) Risk analysis for 2020. Luxembourg: Publications Office of the European Union, p. 56.
- Gabor Kemeny (2020) A qualitative analysis of the hindering and supporting factors of the cross-border information exchange conducted by the Single Point of Contact and the Police and Customs Cooperation Centre.
- Global legal monitor (2018) Italy: New Law on the Protection of Judicial Witnesses Enters into Force.
- Grabosky, P. (2013) Organised Crime and the Internet, The RUSI Journal, 158:5, 18-25, DOI: 10.1080/03071847.2013.847707.
- Heneghan, T (2016) Almost 50 “hot pursuit” police chases stalled at the border, Irish Independent.
- Huybreghts, G. (2015). The Schengen Convention and the Schengen acquis: 25 years of evolution. ERA Forum. 16. 10.1007/s12027-015-0402-3.

- ICMPD (2010) Study on the status of information exchange amongst LEAs in the context of existing EU instruments.
- Interpol (2020) Artificial intelligence and law enforcement: challenges and opportunities.
- Interpol/Unicri (2020) Towards responsible AI innovation.
- Interpol/Unicri (2019) Artificial intelligence and robotics for law enforcement.
- Kleiven, M. E. (2012) Nordic Police Cooperation. In Hufnagel, S., Harfield, C., Bronitt, S. (Eds.), *Cross-border Law enforcement: Regional Law Enforcement Cooperation – European, Australian and Asia Pacific Perspectives*. London: Routledge.
- Levi, M., M. Innes, P. Reuter & Gundur R. (2013) *The Economic, Financial & Social Impacts of Organised Crime in the EU*.
- Meško, G., Furman, R. (2014) Police and prosecutorial cooperation in responding to transnational crime, pp. 323-352, Los Angeles: Sage.
- Microsoft input to the Police Cooperation Code (November 2020). (Not publicly available).
- Milieu Ltd (2018) Assessing the completeness and conformity of Member States measures to transpose Council Framework Decision 2006/960/JHA. (Unpublished).
- Oxford Research, Coffey, Economisti associati, We do-IT (2019) Mid-term evaluation of the Customs 2020 programme - Final report.
- Paoli, L. and Fijnaut C. (2004) General introduction. In: *Organised Crime in Europe: Concepts, Patterns and Control Policies in the European Union and Beyond* C. Fijnaut and L. Paoli (eds.) Dordrecht: Springer.
- RAND Europe & EY for the EC (2021) Mapping the risk of serious and organised crime infiltrating legitimate businesses.
- Sallavaci, O. (2018) Strengthening cross-border law enforcement cooperation in the EU: the Prüm network of data exchange. *Eur J Crim Policy Res* 24, 219–235.
- Saskia H. (2012) Harmonising police cooperation laws in Australia and the European Union: the tension between local/national and national/supranational interests, *Australian Journal of Forensic Sciences*, 44:1, 45-62, DOI: 10.1080/00450618.2011.581249.
- Spapens, T. (2010) Cross-border public order policing in the Dutch border areas. In: *Policing in Europe*, Antoinette Verhage (ed.) Antwerpen: Maklu-Uitgevers, p. 163-180.
- Spapens, T. (2015) Transnational organised crime. *International Encyclopedia of the Social & Behavioral Sciences (Second Edition)*, pp. 596-601.
- Stevnsborg, H. (2019), Nordic Police Cooperation. In McDaniel, J. L., Stonard, K. E., Cox, D. J. (Eds.), *The Development of Transnational Policing*. London: Routledge, DOI: 10.4324/9781351039543.
- Tait R. (2019) Prague prepares for England fans' long weekend with 'anti-conflict units'. *The Guardian*.
- The Brussels Times (2018) Hackers steal personal details of 64,000 Tomorrowland visitors.
- The Guardian (2019) Sinking city: how Venice is managing Europe's worst tourism crisis.
- UNODC and Unicri (2005) *Trends in Crime and Justice: The evolving challenge of transnational organised crime*.

VOA (2021) Along with COVID, France's Hospitals Battle Cyberattacks.

Vox (2019) Game of Thrones tourism is wildly popular – and not just because the show is a hit.

Wagner J. (2021) Transnational Organised Crime (TOC). In: Border Management in Transformation. Advanced Sciences and Technologies for Security Applications. Springer, Cham.

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at:

https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- at the following standard number: +32 22999696, or
- by email via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications from: <https://op.europa.eu/en/publications>.

Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex at: <http://eur-lex.europa.eu>

Open data from the EU

The official portal for European data (<https://data.europa.eu/en>) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

