JUST-2024-JCOO

Justice Programme (JUST)

GA No. 101192923

INCEPT: Supporting cross-border judicial cooperation in cases related to INterCEPTion of telecommunications

INCEPT

WP2: Data Collection & INCEPT Methodology

D2.1: Report with collected and analysed data

WP2 leader: Znanstveno-raziskovalno središče Koper

ZRS Koper 2025

Funded by the European Union

This deliverable was funded by the European Union under Grant Agreement 101192923. The content of this report, including views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the European Commission can be held responsible for them.

Acronym	**INCEPT**
Title	Supporting cross-border judicial cooperation in cases related to INterCEPTion of telecommunications
Coordinator	Law and Internet Foundation
GA No.	101192923
Programme	Justice Programme (JUST)
Topic	JUST-2024-JCOO
Start	1 January 2025
Duration	24 months
Consortium	Law and Internet Foundation (LIF), Bulgaria Adam Mickiewicz University Poznań (AMU), Poland CEELI Institute (CEELI), Czechia Science and Research Centre of Koper (ZRS Koper), Slovenia

Dissemination level		
PU	Public	X
SEN	Sensitive, limited under the conditions of the Grant Agreement	
EU - R	RESTREINT-UE/EU-RESTRICTED under Decision 2015/444	
EU - C	CONFIDENTIEL-UE/EU-CONFIDENTIAL under Decision 2015/444	
EU - S	SECRET-UE/EU-SECRET under Decision 2015/444	
Document version control:		
	Author(s)	**Date**
Version 1	**Drafted by:** ZRS Koper: Benjamin Flander, Erazem Bohinc, Anže Erbežnik, Martin Jančar, Rade Trivunčević **Based on inputs (case-law and normative analysis) from:** LIF: Martina Bogdanova AMU: Zofia Branicka, CEELI: Marek Svoboda	27 July 2025
Version 2	Edited by: LIF: Rada Stoilova; AMU: Martyna Kusak, Weronika Raniszewska	29 July 2025
Version 3	Updated by: ZRS Koper: Benjamin Flander, Erazem Bohinc, Anže Erbežnik, Martin Jančar, Rade Trivunčević	5 August 2025
Version 3	Reviewed by: LIF: Rada Stoilova	5 August 2025

Table of Contents

Abstract i

Table of Abbreviations ii

Glossary iv

1. INTRODUCTION: SUPPORTING CROSS-BORDER JUDICIAL COOPERATION IN CASES RELATED TO INTERCEPTION OF TELECOMMUNICATIONS 1

2. AIM OF THE STUDY 4

3. METHODOLOGY AND THE STRUCTURE OF THE REPORT 5

4. THE STATE OF THE ART 6

4.1. Literature review 6

4.1.1 Basic perspectives on global and cross-border dimensions of telecommunications interception 6

4.1.2 EIO Directive and cross-border exchange of evidence 7

4.1.3 Comparative and National Perspectives 8

4.1.4 Infrastructural, Technological, Market, and Regulatory Challenges 10

4.1.5 Encrypted Communications, Admissibility, and Case Law 11

4.1.6 Synthesis and Gaps 11

4.2. EU funded projects 12

4.3. Other projects 22

5. EUROPEAN UNION FRAMEWORK 26

5.1. Council Resolution on the lawful interception of telecommunications 27

5.2. Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union 28

5.3 Directive 2014/41/EU on the European Investigation Order 29

5.3.1 The European Investigation Order and the scope of the EIO Directive 29

5.3.2 The structure and content of the EIO Directive 30

5.3.3 Specific provisions on the interception of telecommunications 31

5.4 Roadmap for lawful and effective access to data for law enforcement 33

6. NATIONAL LEGAL FRAMEWORKS 36

6.1. Slovenia 36

6.1.1 Provisions on the interception of telecommunications 36

6.1.1.1 Constitutional review of the Criminal Procedure Act provisions related to telecommunications interception 38

6.1.1.2 The 2024 amendments to the Slovenian Criminal Procedure Act (CPA-P) 40
6.1.1.3 The Electronic Communications Act (ZEKom-2) 46
6.1.1.4 Oversight and control 46
6.1.1.5 Summary and conclusion 48
6.1.2 Provisions on cross-border judicial cooperation related to interception of telecommunications 49
6.1.2.1 The Act on Cooperation in Criminal Matters with Member States of the European Union 49
6.1.2.2 The European Investigation Order 50
6.1.2.3 The European Investigation Order for the surveillance of telecommunications 51
6.1.2.4 EIO statistics 53
6.2. Bulgaria 55
6.2.1 Provisions on the interception of telecommunications 56
6.2.1.1 Overview of the legal framework 56
6.2.1.2 Special intelligence means and telecommunications interception 56
6.2.1.3 Legal admissibility and oversight 59
6.2.1.4 Constitutional review of the Electronic Communications Act and the Special Intelligence Means Act provisions related to telecommunications interception 59
6.2.2 Provisions on cross-border judicial cooperation related to interception of telecommunications 60
6.2.2.1 The Law on the European Investigation Order 60
6.2.2.2 Issuing and executing EIOs in cases involving telecommunications interception 60
6.2.2.3 EIO statistics 61
6.3. The Czech Republic 62
6.3.1 Provisions on the interception of telecommunications 62
6.3.1.1 Overview of the legal framework 62
6.3.1.2 Covert investigative measures related to communications interception 63
6.3.1.3 Categories of intercepted or accessed data and conditions for the interception 64

6.3.1.4 Time limitations, procedural safeguards, admissibility, remedies, and oversight 64
6.3.1.5 Constitutional review of the Electronic Communications Act and the Special Surveillance Means Act provisions related to telecommunications interception 65
6.3.2 Provisions on cross-border judicial cooperation related to interception of telecommunications 66
6.3.2.1 Act on International Judicial Cooperation in Criminal Matters 66
6.3.2.2 Issuing and executing EIOs in cases involving covered investigative measures, including telecommunications interception 67
6.3.2.3 EIO statistics 68
6.4. Poland 68
6.4.1 Provisions on the interception of telecommunications 68
6.4.1.1 Overview of the legal framework 68
6.4.1.2 Categories of covert investigative measures related to communications interception 70
6.4.1.3 Procedure and prerequisites for the interception of telecommunications 71
6.4.1.4 Time limitations 73
6.4.1.5 Procedural issues of telecommunications interception and admissibility of evidence 74
6.4.1.6 Constitutional review of the Electronic Communications Act and the Special Surveillance Means Act provisions related to telecommunications interception 76
6.4.2 Provisions on cross-border judicial cooperation related to interception of telecommunications 77
6.4.2.1 Provisions of the Code of Criminal Procedure on EIO in cases involving communications interception 77
6.4.2.2 Issuing and executing EIOs in cases involving covered investigative measures, including telecommunications interception 77
6.4.2.3 EIO statistics 78
7. CASE LAW 80
7.1. ECtHR case law 80
7.1.1 Definition of privacy 80
7.1.2 ECtHR standing of applicants regarding secret surveillance 81

7.1.3 Article 8 ECHR tri-partite test 82
7.1.3.1 In accordance with the law 83
7.1.3.2 Necessary in a democratic society 84
7.1.3.3 Targeted interception v. bulk interception 85
7.1.4 Relationship between Articles 6 and 8 ECHR regarding fairness of proceedings and admissibility of evidence 87
7.2. CJEU case law 88
7.2.1 Telecommunication data retention 88
7.2.1.1 Prohibition of general and non-discriminate systems 89
7.2.1.2 Targeted systems 90
7.2.1.3 Authorisation authorities 91
7.2.1.4. Admissibility of evidence 91
7.2.2 EU-US data transfers 91
7.3. National case law 92
7.3.1 Slovenia 92
7.3.1.1 Use of Telecommunications Interception in Jurisprudence 92
7.3.1.1.1 Constitutional Framework and covered investigative measures 92
7.3.1.1.2. Judicial Authorisation and Procedural requirements 93
7.3.1.1.3 Catalogue of Qualifying Offences and Proportionality 94
7.3.1.1.4 Safeguards and Procedural Protections 95
7.3.1.2 Use of Evidence Obtained Abroad 96
7.3.1.2.1 Mutual Legal Assistance Framework 96
7.3.4.2.2 Admissibility Standards for Foreign Evidence 96
7.3.1.3 Synthesis: Implications for Cross-Border Judicial Cooperation 99
7.3.2 Bulgaria 99
7.3.2.1 Use of Telecommunications Interception in Jurisprudence 99
7.3.2.1.1 Constitutional Framework and Special Intelligence Means 99
7.3.2.1.2 Judicial Authorisation and Procedural Requirements 100
7.3.2.1.3 Evidence Standards and Admissibility 100
7.3.2.1.4 Professional Privilege and Protected Communications 100
7.3.2.2 Use of Evidence Obtained Abroad 101

7.3.2.2.1 European Investigation Orders and Procedural Compliance 101
7.3.2.2.2 European Court of Human Rights Jurisprudence 101
7.3.2.2.3 Court of Justice of the European Union Cases 101
7.3.2.2.4 Administrative Court Oversight 102
7.3.2.3 Synthesis: Implications for Cross-Border Judicial Cooperation 102
7.3.3 Poland 103
7.3.3.1 Use of Telecommunications Interception in Jurisprudence 103
7.3.3.1.1 Catalogue of Qualifying Offences and Proportionality 103
7.3.3.1.2 Safeguards and Procedural Protections 104
7.3.3.2 Use of Evidence Obtained Abroad 104
7.3.3.2.1 Mutual Legal Assistance Framework 104
7.3.3.2.2 Admissibility Standards for Foreign Evidence 104
7.3.3.2.3 Third-Party Protection in Cross-Border Context 105
7.3.3.3 Synthesis: Implications for Cross-Border Judicial Cooperation 105
8. CHALLENGES AND BEST PRACTICES IN CROSS-BORDER INTERCEPTION OF TELECOMMUNICATIONS IN THE EUROPEAN UNION 107
8.1 The scope of the EIO Directive and the meaning and scope of 'interception of telecommunication' 107
8.2 Content and form 110
8.2.1 Filling in the EIO (Annexes A, B and C) 110
8.2.2 Information or documents to be – or not to be – provided by the issuing authority 110
8.2.3 Language 111
8.3 Issuing and transmitting 111
8.3.1 Issuing and validating authority (verifying an incoming EIO on telecommunications interception) 111
8.3.2 Proportionality check, consultation mechanism, and costs 111
8.3.3 Multiple measures 112
8.3.4 Transmission 112
8.4 Recognition and execution 113
8.4.1 Competent authorities 113
8.4.2 Recognition and execution 113
8.4.3 Differences in national legal frameworks 114

8.4.4 Recourse to a different type of investigative measure 117
8.4.5 Incompatibility with the obligations regarding fundamental rights and other grounds for non-recognition or non-execution 117
8.4.6 Challenges and best practices in urgent cases 118
8.4.7 Acknowledgement of receipt and time limits 118
8.4.8 Rule of speciality 119
8.4.9 EIO and cross-border surveillance 119
8.5 Challenges related to specific provisions on interception of telecommunications (Articles 30 and 31) 119
8.5.1 Interception of telecommunications with technical assistance 119
8.5.2 Interception of telecommunications without technical assistance 120
8.6 Other challenges identified by Eurojust and the EJN 122
8.6.1 The description of the investigative measure requested 122
8.6.2 Domestic judicial decision authorising a coercive investigative measure 122
8.6.3 Use of the investigative measure restricted to certain offences 122
9 ENCROCHAT AND SKY ECC: CROSS-BORDER EVIDENCE GATHERING THROUGH MASS INTERCEPTION OF ENCRYPTED COMMUNICATIONS 123
9.1 The EncroChat case 123
9.2 The Sky ECC case 126
10 RECOMMENDATIONS FOR THE INCEPT PROJECT 129
11 CONCLUSION 135
12 BIBLIOGRAPHY 136

List of Tables

Table 1: Communications interception in Slovenia (competent authorities, standards of proof, duration) 44
Table 2: Number of EIOs issued and received by the State Prosecutor's Office (Slovenia) 54
Table 3: Number of EIOs issued and received by courts (Slovenia) 55
Table 4: Duration of communications interception 58
Table 5: Number of outgoing EIOs (Bulgaria) 61
Table 6: Number of incoming EIOs (Bulgaria) 61
Table 7: Interception of telecommunications – similarities and differences between countries 114

Abstract

This report serves as Deliverable D2.1 of Work Package 2 (WP2), 'Data Collection & INCEPT Methodology,' within the INCEPT project, funded by the European Commission's Justice Programme. The mission of the INCEPT project, launched in January 2025 and implemented by a consortium from Bulgaria, Poland, the Czech Republic, and Slovenia, is, *inter alia*, to map legal frameworks, practices, and challenges in implementing European Investigation Orders (EIOs) for intercepting communications like phone calls, messaging services, emails and messaging apps such as Skype, WhatsApp, Viber, Telegram etc. Furthermore, the INCEPT project focuses on enhancing cross-border judicial cooperation among EU Member States, particularly in implementing the EIOs for cases involving telecommunications interception. By employing diverse research methods, INCEPT project aims to map similarities, differences, best practices, and challenges in Central and Eastern Europe, ultimately developing an INCEPT Methodology and INCEPT Manual for judges, prosecutors, investigators, and defence lawyers to balance the law enforcement needs with fundamental rights protection, drawing on EU instruments like the EIO Directive and relevant case law.

The core analysis includes a structured literature review synthesising EU and global perspectives on surveillance governance, detailed examinations of EU and national legal regimes, and case law overview. Key findings reveal persistent challenges in the cross-border interception of telecommunications via EIOs in countries participating in the INCEPT project: divergent authorisation authorities, prerequisites and thresholds, offence catalogues, procedural safeguards, technical standards, duration limits, and admissibility issues for cross-border evidence, as well as gaps in handling technologies like IMSI catchers and Trojan horses.

The report concludes by examining the cross-border evidence gathering through mass interception of encrypted telecommunications – arguably one of the most sensitive and controversial aspects of criminal investigations – and by presenting recommendations for further research and guidance for implementing the activities and tasks within the INCEPT project.

Overall, cross-border cooperation in telecommunications interception is a legally and technically complex issue, vital for the successful prevention, detection, investigation, and prosecution of crime, as well as for ensuring security in the EU. While the Union has made significant progress through legal instruments such as the EIO and the work of support bodies like Eurojust and the European Judicial Network, further steps are needed. Strengthening bilateral, multilateral, and multi-jurisdictional cooperation between Member States, alongside harmonisation efforts and rights-based reforms, is essential to building a trusted and effective framework for cross-border interception of telecommunications.

Table of Abbreviations

ASIO	Australian Security Intelligence Organisation
CCP	Code of Criminal Procedure
CJEU	Court of Justice of the European Union
CIM	Covert Investigative Measures
CPA	Criminal Procedure Act (used in several national contexts)
CoE	Council of Europe
CPC	Criminal Procedure Code
DPA	Data Protection Authority
EAW	European Arrest Warrant
ECtHR	European Court of Human Rights
ECHR	European Convention on Human Rights
EIO	European Investigation Order
EJN	European Judicial Network
EU	European Union
GDPR	General Data Protection Regulation
GIC	Groupement Interministériel de Contrôle (France)
IMSI	International Mobile Subscriber Identity
JIT	Joint Investigation Team
JUST	Justice Programme (European Commission funding programme)
LEA	Law Enforcement Agency
LSIM	Law on Special Intelligence Means (Bulgaria)
MLA	Mutual Legal Assistance
MLAR	Mutual Legal Assistance Regulation

NCIS	National Criminal Intelligence Service
NGO	Non-Governmental Organisation
OVS MORS	Intelligence and Security Service at the Ministry of Defence (Slovenia)
PP	Pravna praksa (Slovenian legal journal), or sometimes Public Prosecutor
SANS	State Agency for National Security (Bulgaria)
SOVA	Slovene Intelligence and Security Agency
SIM (BG context)	Special Intelligence Means (Bulgaria)
SSRN	Social Science Research Network
VPN	Virtual Private Network
WP	Work Package
ZEKOM-2	Electronic Communications Act (Slovenia)
ZRS Koper	Science and Research Centre Koper (Slovenian project partner)

Glossary

1. **Competent authority**

The designated national body responsible for issuing, receiving, or executing cross-border requests for judicial cooperation, including EIOs for telecommunications interception. May be judicial, prosecutorial, or administrative depending on national law.

2. **Covert Investigative Measures (CIM)**

Secret investigative techniques used by law enforcement to gather evidence without the knowledge of suspects, including telecommunications interception, surveillance, and undercover operations. Subject to strict procedural safeguards and judicial authorisation.

3. **Cross-border surveillance**

Surveillance activities that span multiple jurisdictions and require coordination between law enforcement agencies of different countries and compliance with various national legal frameworks. Often facilitated through EIOs or MLA requests.

4. **Electronic evidence (E-Evidence)**

Digital information and data stored or transmitted in binary form that may be relied upon as evidence in criminal proceedings, including intercepted communications and metadata. Subject to specific admissibility and procedural requirements.

5. **European Investigation Order (EIO)**

A judicial decision which has been issued or validated by a judicial authority of a Member State to have one or several specific investigative measure(s) carried out in another Member State to obtain evidence in accordance with Directive 2014/41/EU. The EIO may also be issued for obtaining evidence that is already in the possession of the competent authorities of the executing State.

6. **IMSI catcher**

A surveillance device that acts as a fake mobile phone tower (base station) to intercept mobile communications and track location data by tricking nearby mobile phones into connecting to it rather than legitimate cell towers. It is used by law enforcement agencies with proper judicial authorisation to identify the International Mobile Subscriber Identity (IMSI) and location of mobile devices.

7. **Judicial authority**

According to CJEU case law, authorities participating in the administration of criminal justice in a Member State, acting independently in the exercise of their responsibilities and under procedures complying with effective judicial protection requirements. This includes judges, courts, and certain public prosecutors who meet independence criteria from executive influence.

8. **Judicial cooperation**

Collaboration between judicial authorities of different countries in criminal matters, including sharing evidence, executing arrest warrants, and conducting joint investigations. Facilitated by instruments like the EIO.

9. Lawful interception

The facilities in telecommunications networks that allow law enforcement agencies with court orders or other legal authorisation to selectively wiretap individual subscribers. It refers to obtaining communications network data pursuant to lawful authority for the purpose of analysis or evidence.

10. Metadata (Telecommunications)

Data that provides information about other data, specifically information processed for the purposes of transmitting, distributing or exchanging electronic communications content, including data used to trace and identify the source and destination of communications, location data, and timing information. It does not include the actual content of communications.

11. Mutual Legal Assistance (MLA)

The formal process of cooperation between two or more countries for gathering and exchanging information in an effort to enforce public or criminal laws. It involves the provision of legal assistance by one state to another in the investigation, prosecution, or punishment of criminal offences.

12. Real-time interception

The immediate capture and monitoring of telecommunications content and metadata as communications occur, requiring technical capabilities to intercept and analyse data without delay or as of transmission. Distinguished from accessing stored historical data.

13. Special Intelligence Means (SIM)

Technical devices and operational methods used to gather evidence in serious criminal investigations, including electronic surveillance, wiretapping, and covert monitoring activities. Regulated under specific national legislation with judicial oversight requirements.

14. Technical means

Electronic devices, mechanical devices, and software used to record and monitor the activities of suspected persons and their communications, including wiretapping equipment and surveillance technology. Must be legally authorised and technically certified for use in criminal investigations.

15. Telecommunications traffic data

Information processed for the purpose of conveying communications on an electronic communications network, including location data, subscriber information, and technical routing data. Distinct from communication content.

16. Trojan horse (Computing/Surveillance)

A type of malicious software that disguises itself as a legitimate program to gain unauthorised access to computer systems. In the law enforcement context, it refers to covert software used to monitor electronic communications and data on target devices, requiring proper judicial authorisation for lawful use.

1. INTRODUCTION: SUPPORTING CROSS-BORDER JUDICIAL COOPERATION IN CASES RELATED TO INTERCEPTION OF TELECOMMUNICATIONS

This report is Deliverable D2.1 of Work Package 2 (WP2), »Data Collection & INCEPT Methodology« of the INCEPT project, »Supporting Cross-Border Judicial Cooperation in Cases Related to Interception of Telecommunications« funded by the European Commission under the JUST Programme. The project is implemented by an international consortium comprising four partner organisations based in Bulgaria, Poland, the Czech Republic, and Slovenia.[1]

Launched in January 2025, INCEPT focuses on judicial cooperation among EU Member States, particularly regarding the implementation of the European Investigation Order (EIO) in cases involving telecommunications interception in criminal investigations. The project aims to develop a Methodology and a Manual specifically for actors involved in the criminal process.

Using multiple research methods and approaches in data collection and analysis, INCEPT targets four Central and Eastern European countries to map similarities, differences, and both best and worst practices in the region concerning cross-border telecommunication interception through the application of the EIO.

An innovative aspect of the project's outputs is the focus on telecommunication interception in criminal investigations, in addition to covering key elements of the general implementation of the EIO. The project includes capacity-building activities at both national and international levels for judges, prosecutors, investigators, and legal practitioners (particularly defence lawyers) to enhance their professional knowledge and skills in the context of telecommunication interception and some other problematic areas of the EIO.

By combining diverse methods and approaches, INCEPT aims at enhancing both the level of judicial cooperation and the effective implementation of the EIO in criminal matters involving telecommunication interception, ensuring its proper application and the admissibility of the evidence collected through it.

The interception of telecommunications – such as telephone calls, messaging services, emails, social media, and other electronic communications – is an essential tool in criminal investigations, particularly in combating terrorism, organised crime, and cybercrime. Specific provisions on the interception of telecommunications are found in the criminal procedure laws of Member States, typically within the sections on covert investigative measures.

In EU law, explicit provisions on the interception of telecommunications can be found in instruments on judicial cooperation between Member States, such as the 2000 MLA Convention[2] and the EIO Directive.[3] However, there is no unified EU regulation governing covert investigative measures in general, nor surveillance and interception of telecommunications in particular. Over the past decade, national laws, international law, and EU law, including case law of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU), have

[1] Adam Mickiewicz University in Poznań (Poland), the CEELI Institute (Czech Republic), the Science and Research Centre Koper (Slovenia), and the Law and Internet Foundation (Bulgaria), the latter serving as the project's lead partner.
[2] Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union OJ C197/3.
[3] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130.

raised several questions concerning various aspects of telecommunication interception and monitoring.

Guidance to practitioners on cross-border gathering of evidence with investigative measures including interception of telecommunications through the EIO mechanism, was provided by Eurojust and the European Judicial Network (EJN) in their 2019 Joint Note on the practical application of the EIO.[4] This document is a compilation of information, highlighting issues, challenges, possible solutions and best practices. It addresses identified issues related to the four main phases of the lifecycle of an EIO (the issuing phase, the transmission phase, the recognition phase and the execution phase), as well as issues related to the scope of the EIO Directive, its use vis-à-vis other co-existing legal instruments, the competent authorities, the content, form and language of the EIO and the use of some specific investigative measures including the interception of telecommunications. This document compiles information on the key issues, challenges, potential solutions, and best practices concerning the EIO. It covers all four phases of the EIO lifecycle (e.g., issuing, transmission, recognition, and execution) while also addressing matters related to the Directive's scope, its interaction with other legal instruments, the role of competent authorities, requirements for content, form, and language, and the use of specific investigative measures, including telecommunications interception.[5] Another important 'guidance' document is Eurojust's 2020 report on its casework in the field of EIO.[6] This document informs both practitioners and policymakers of the main difficulties encountered in the practical application of the European Investigation Order (EIO) on the basis of Eurojust's casework.

One set of issues referred to by Eurojust and the EJN relates to the scope of the EIO Directive. At the EU level, there is no uniform interpretation of the terms 'surveillance' or 'interception' of telecommunications, nor is there explicit regulation of certain surveillance measures – such as audio-video surveillance in private spaces requested in one Member State and executed in another, GPS tracking initiated in the issuing Member State and crossing a border, or surveillance through Trojan-horse-like software installed on a portable electronic device that crosses a border.

In principle, the EIO Directive applies to the cross-border execution of any type of investigative measure intended to gather or use evidence ordered by a judicial authority, with the exception of the establishment of joint investigation teams and cross-border surveillance, as referred to in the Convention implementing the Schengen Agreement. Given this broad scope, the EIO Directive could apply to the aforementioned surveillance measures, provided that the purpose of the requested measures is to gather evidence and that a judicial authority has issued or validated them.[7]

Accordingly, it can be asked whether the aforementioned measures fall under the general regime of the EIO Directive or under the specific provisions related to the interception of telecommunications (Articles 30-31 of the EIO Directive). For each of these measures, further questions arise, such as whether Annex A or Annex C of the EIO Directive must be used, whether

[4] Eurojust and European Judicial Network, 'Joint Note on the Practical Application of the European Investigation Order' (June 2019) https://www.eurojust.europa.eu/sites/default/files/assets/eurojust_ejn_joint_note_practical_application_european_investigation_order.pdf accessed 31 July 2025.
[5] *Ibid.*, p. 5.
[6] Eurojust, 'Report on Eurojust's casework in the field of the European Investigation Order' (November 2020) https://www.eurojust.europa.eu/sites/default/files/assets/2020_11_eio_casework_report_corr.pdf accessed 3 August 2025.
[7] See n 4, p. 15. According to Eurojust and the EJN's Joint Note, different views prevail concerning whether Article 30 of the EIO Directive could be applied to a request to install a covert listening device (e.g., 'bugging' of a car).

ex-post notification is possible, what specific conditions apply under national law, which authorities are competent, and so on.

Another series of issues referred to by Eurojust and the EJN follows from differences in national legal provisions and technical standards on the interception of telecommunication. Some of the issues arising in this area are differences in the prerequisites for issuing and the duration of the interception in the respective Member States (i.e. thresholds, competent authorities, possibilities of an extension, time frames etc.) and technical possibilities to channel the intercepted conversations in real-time to the issuing authority in accordance with Article 30(6) of the EIO Directive.

Like the MLA regime, the EIO system operates without prior harmonisation of rules on the admissibility of evidence. After the entry into force of the EIO Directive, which largely replicated the relevant provisions of the 2000 MLA Convention, disparities in national legislation, the cross-border nature of both crime and digital communication, divergent interpretations of privacy and other fundamental rights, as well as technical challenges, continue to pose significant difficulties for EU institutions. Therefore, issues resulting from differences in national laws, which existed under the MLA regime, continue to exist under the mutual recognition regime.[8]

Interception of telecommunications in criminal investigations is also highlighted in the Joint Factsheet of the Registry of the European Court of Human Rights and the European Union Agency for Fundamental Rights (FRA). In view of recent technological and social developments in the sphere of electronic communications, the ECtHR and the CJEU have been called upon to address the risks to human rights stemming from mass surveillance regimes (e.g., systems allowing large-scale technical collection of information) in and related to electronic communications. Mass surveillance may target the content of electronic communications and/or related communication data, including subscribers' and registered users' personal data as well as traffic and location data. As to the content of electronic communications, a particular set of issues may arise when the bulk interception, retention and access thereof include the national authorities' attempts to decrypt encrypted electronic messages.[9]

Overall, cross-border cooperation related to telecommunications interception is a legally and technically complex issue, essential for the successful prevention, detection, investigation, and prosecution of crime, as well as for ensuring security in the EU. However, it must be carefully balanced with fundamental rights and the rule of law. While the EU has made significant progress through legal instruments such as the EIO and support bodies like Eurojust and the EJN, further bilateral and multilateral/multi-jurisdictional cooperation, as well as harmonisation and rights-based reforms, are essential to building a trusted and effective framework for lawful interception of telecommunications between Member States.

[8] See n 6, p. 23.
[9] Case C-670/22 *M.N. (EncroChat)* EU:C:2024:372 and Podchasov v Russia App no 33696/19 (ECtHR, 13 February 2024). See also: Registry of the European Court of Human Rights and European Union Agency for Fundamental Rights, 'Mass surveillance: ECtHR and CJEU Case-Law, Joint Factsheet' (February 2025), https://ks.echr.coe.int/documents/d/echr-ks/mass-surveillance accessed 2 August 2025, p. 2.

2. AIM OF THE STUDY

In the context described above, T2.1 »Research and Data Analysis«, coordinated by the Science and Research Centre Koper (ZRS Koper), aims to conduct secondary research and identify existing knowledge and challenges in the field of cross-border judicial cooperation in the EU related to telecommunications interception through the application of the EIO. This includes findings from previous EU-funded and other relevant projects, as well as existing literature, reports, legal frameworks, and case law in the field.

The collection and analysis of this data will inform the development of the Measures-related questionnaire (T2.2) and the INCEPT Methodology (T2.3), by integrating analysis of literature, legal frameworks, and case law at both national and EU levels. This process will help identify current gaps and challenges, as well as potential best practices, in the cross-border interception of telecommunications via the EIO mechanism. Each partner is responsible for conducting the research at the national level, while ZRS Koper oversees the data at the European level, coordinates the overall process, and prepares the report as project deliverable D2.1.

The research conducted under T2.1 uses a desktop research methodology (a secondary research method). This approach allows for the use of existing data to establish a foundation for further research, define its scope, and formulate relevant questions and research areas. It serves as a preparatory step before the implementation of national capacity-building activities (T3.1–T3.4) in each project partner country, international capacity-building activities (T3.5) – which include two one-day international events in Poland and Bulgaria – and the development of the Manual on cross-border judicial cooperation related to the use of telecommunications interception (T4.2).

Relevant data has been obtained from a wide range of sources. EU-funded projects were identified using the CORDIS database, with information collected from project websites and their publicly available deliverables. The literature review was conducted using open-access sources as well as public or private databases.

The survey focuses on the legal dimensions of cross-border telecommunications interception, while ethical and technical considerations of lawful interception fall outside the scope of this report (for the technical aspects of lawful interception, see the publications listed in Section 4.1.4). Regarding legal aspects, normative and comparative methods of legal analysis have been applied. This includes accessing national legal sources through official gazettes and both public and private legal information systems in each project partner country, as well as consulting EU legal acts and other Union legal sources via EUR-Lex. The secondary research is limited to the period from 2015 to 2025.

3. METHODOLOGY AND THE STRUCTURE OF THE REPORT

Focusing on cross-border judicial cooperation in cases related to the interception of telecommunications, this report – and the secondary research underpinning it – addresses legal and practical considerations surrounding the interception of telecommunications via phone calls and SMS messages, as well as the collection of real-time electronic data and evidence transmitted across telecommunications networks managed by electronic communications service providers registered in either domestic or foreign jurisdictions.

The report also examines issues related to the collection of electronic data and evidence through mass surveillance techniques, particularly in the context of real-time interception and monitoring. However, it does not cover data and evidence stored on suspects' or third parties' electronic devices or within online information systems, including computers, smartphones, tablets, smartwatches, electronic appliances, portable media, and cloud storage. Additionally, the report does not explore the use of AI systems or strategies such as Predictive Risk Assessment or other similar approaches aimed at crime prevention and the enhancement of law enforcement capabilities.

Considering the issues outlined in Section 1, the report begins with a brief overview of selected EU-funded and other projects, as well as scientific literature relevant to telecommunications interception, with a particular focus on cross-border judicial cooperation within the EU. It then analyses the EU and national legal frameworks and relevant case law in the four participating countries, along with the applicable Council of Europe (CoE) and EU jurisprudence.

Shifting focus to the challenges and best practices in cross-border telecommunications interception through the EIO mechanism, the report explores, among other things, the scope of the EIO Directive, the meaning of the term 'interception of telecommunication,' content and form of the EIO, the four main phases of an EIO's lifecycle (e.g., issuance, transmission, recognition, and execution), inconsistencies in national laws on lawful interception, and challenges related to specific provisions on interception of telecommunications (Articles 30-31 of the EIO Directive).

A dedicated section briefly examines EncroChat and Sky ECC, landmark cases involving high-profile cross-border criminal investigations and the decryption of secure communication platforms used by criminal networks. Based on an indiscriminate bulk data interception of telecommunications, these cases raise significant legal and ethical challenges.

The report concludes with recommendations for further research, as well as guidance for implementing the activities and tasks within the INCEPT project.

4. THE STATE OF THE ART

4.1. Literature review

This section provides a structured overview of key literature relevant to the cross-border judicial cooperation in the EU related to telecommunications interception through the application of the EIO. To identify relevant literature, an extensive search was conducted using the open-access academic and professional sources, such as *Google Scholar*, *Oxford Academic*, *SSRN* and others. The search employed targeted keywords including interception of telecommunications, cross-border judicial cooperation, European Investigation Order, and electronic evidence.

The literature review revealed an abundance of resources on telecommunications interception. However, there is a significant lack of studies specifically focused on cross-border judicial cooperation in cases involving telecommunications interception. This report seeks to incorporate the most relevant resources from both fields.

4.1.1 Basic perspectives on global and cross-border dimensions of telecommunications interception

The book Crime in the Digital Age (Grabosky, Smith, Wright)[10] includes the chapter 'Illegal Interception of Telecommunications', which offers an in-depth examination of the legal and practical issues surrounding unauthorised interception activities. It discusses the various forms of illegal interception, the motivations behind such acts, and the difficulties faced by law enforcement in detecting and prosecuting offenders. The chapter also addresses the implications of illegal interception for privacy rights and the integrity of communications systems, reinforcing the necessity for clear legal definitions and effective enforcement strategies to protect individuals and institutions from unlawful surveillance.

The article Regulating Telecommunications Interception and Access in the Twenty-first Century: Technological Evolution or Legal Revolution? (Bronitt, Stellios)[11] provides a critical analysis of how rapid technological advancements have outpaced existing legal frameworks governing telecommunications interception. The authors argue that the evolution of interception technologies has created significant regulatory challenges, requiring not only updates to legal provisions but also a rethinking of the balance between security imperatives and civil liberties. The article highlights the need for legal systems to adapt to new forms of communication and interception, emphasising the importance of both technological literacy and robust oversight mechanisms in the regulatory process.

Adding to the foundational context on the governance and power dynamics of electronic networks is work by Drake and Wilson's edited volume, Governing Global Electronic Networks: International Perspectives on Policy and Power[12]. This book explores the international policy frameworks and power structures that underpin electronic communications, providing essential context for understanding the global and cross-border dimensions of telecommunications interception.

[10] Grabosky, P. N., Smith, R. G. and Wright, P., *Crime in the Digital Age* (Routledge 1998).
[11] Bronitt, S. and Stellios, J., 'Regulating Telecommunications Interception and Access in the Twenty-first Century: Technological Evolution or Legal Revolution?' (2006) 24 Prometheus 413.
[12] Drake, W. J. and Wilson III, E. J. (eds), *Governing Global Electronic Networks: International Perspectives on Policy and Power* (MIT Press 2008).

The broader societal and ethical implications of surveillance are further examined in Law, Surveillance and the Humanities (Brunon-Ernst, Gligorijevic, Manderson, eds.)[13] and Surveillance, Privacy and Public Space (Newell, Timan, Koops, eds.)[14]. These collections analyse how surveillance practices intersect with fundamental rights, privacy, and the evolving concept of public and private spaces in the digital era. They underscore the tension between state security interests and individual freedoms, a recurring theme in the literature on telecommunications interception.

4.1.2 EIO Directive and cross-border exchange of evidence

The legal architecture for cross-border interception of telecommunications within the EU is shaped by the EIO Directive, as well as national and international law. Tudorica and Bonnici (2023)[15] provide a comprehensive analysis of the legal framework for digital evidence following the implementation of the EIO Directive, highlighting both the progress made and the persistent challenges and inconsistencies across Member States. Furthermore, it helps understand the practical experiences and legal uncertainties that arise in the application of the EIO to electronic evidence.

Ambos (2024)[16], in Treatise on International Criminal Law, offers a critical examination of international criminal procedure, including the challenges of cross-border evidence collection and the role of judicial cooperation in ensuring fair trial rights. This analysis of procedural safeguards and the interplay between national and supranational legal frameworks provides a foundational perspective for understanding the complexities of telecommunications interception in transnational criminal cases.

Verras and Chapman (2023)[17], drawing on Eurojust's operational reports, delve into the practical problems, solutions, and technical practices associated with the EIO. Their analysis emphasises the '*favor cooperationis*' principle but also documents operational bottlenecks, such as divergent national procedures, technical incompatibilities, and issues related to the admissibility of evidence obtained via cross-border interception.

Zaharieva (2017)[18] offers a practitioner's perspective on the choice between the EIO and Joint Investigation Teams (JITs) as mechanisms for cross-border cooperation, discussing the relative advantages and limitations of each, particularly in complex investigations involving telecommunications data.

[13] Brunon-Ernst, A., Gligorijevic, J., Manderson, D. and Wrobel, C. (eds), *Law, Surveillance and the Humanities* (Edinburgh University Press 2025).
[14] Newell, B. C., Timan, T. and Koops, B.-J. (eds), *Surveillance, Privacy and Public Space* (Routledge 2019).
[15] Tudorica M and Bonnici JM, 'Legal framework for digital evidence following the implementation of the EIO Directive: Status quo, challenges and experiences in Member States' in MA Biasiotti and F Turchi (eds), *European Investigation Order* (vol 55, Springer 2023) 151.
[16] Ambos K, *Treatise on International Criminal Law: Volume III: International Criminal Procedure* (2nd edn, OUP 2024).
[17] Verras P and Chapman P, 'European Investigation Order: Favor cooperationis, operational problems, solutions and technical practices via the report of the Eurojust' (2023) 2 Yearbook of International Enforcement of Criminal Law and Procedure 371.
[18] Zaharieva R, 'The European investigation order and the joint investigation team - which road to take: A practitioner's perspective' (2017) 18(3) ERA Forum 365.

4.1.3 Comparative and National Perspectives

The article Interception of telecommunications for criminal investigation – a comparative analysis by Vassilaki (1994)[19] offers an early but influential examination of how various legal systems approach the interception of telecommunications for criminal investigations. The study systematically compares legislative frameworks, authorisation processes, and oversight mechanisms in different countries, highlighting both convergences and divergences in national practices. It underscores that while some jurisdictions have developed comprehensive statutory regimes with clear procedural safeguards, others rely on more fragmented or less transparent approaches. These disparities can create significant obstacles for mutual legal assistance and the smooth operation of cross-border investigations, particularly when evidence must be shared or recognised across borders.

An additional comparative perspective is offered by a comparative legal analysis provided by Tropina (2021)[20], who examines access to telecommunication data in criminal justice across several jurisdictions. This work identifies significant differences in national approaches to lawful interception, thresholds for authorisation, and procedural safeguards, all of which complicate cross-border cooperation and the effective implementation of the EIO.

National-level studies, such as Polčák et al. (2016)[21] on the Czech Republic and Slovakia, offer detailed insights into the practical realities of implementing interception measures. These works highlight the impact of national legal cultures, institutional arrangements, and technical capacities on the effectiveness of cross-border judicial cooperation.

In Slovenia, Šepec has contributed to this field with an article Mass surveillance of communications: the case of SKY-ECC[22] focusing on mass interception of telecommunications in Slovenia. This article examines the legal framework, constitutional safeguards, and practical challenges related to large-scale surveillance and interception measures, including the requirements for judicial authorisation and the limitations imposed by the Constitutional Court on data retention and surveillance practices. Furthermore, Erbežnik has published a notable article addressing the new EU e-evidence package, EU system for cross-border e-evidence gathering: Regulation (EU) 2023/1543 and Directive (EU) 2023/1544[23]. While this article primarily discusses the mechanisms for cross-border access to electronic evidence stored by service providers, it is important to note that it does not cover the real-time acquisition of electronic data or evidence, but rather focuses on stored data and the procedural rights and safeguards associated with such requests. Furthermore, national intelligence authorities and surveillance in Slovenia are comprehensively analysed by Neža Kogovšek Šalamon in a report for the EU Agency for Fundamental Rights.[24] This study details the legal framework governing the Slovene Intelligence and Security Agency (SOVA) and the Intelligence and Security Service at the Ministry of Defence, outlining the division of competences, the procedures for authorising surveillance, and the safeguards in place to protect fundamental rights. The report highlights the legal framework from

[19] Vassilaki IE, 'Interception of telecommunications for criminal investigation – a comparative analysis' (1994) 10(5) Computer Law & Security Report 238.
[20] Tropina T, 'Comparative analysis' in *Access to Telecommunication Data in Criminal Justice: A Comparative Legal Analysis* (Springer 2021) 11.
[21] Polčák R, Kyncl L and Svoboda D, *Interception of Electronic Communications in the Czech Republic and Slovakia* (Masaryk University 2016).
[22] Šepec M, 'Masovni nadzor komunikacij: primer SKY-ECC' (2025) 44(15) Pravna praksa 6.
[23] Erbežnik A, 'Sistem EU za čezmejno pridobivanje e-dokazov: Uredba (EU) 2023/1543 in Direktiva (EU) 2023/1544' (2024) 26(2) Odvetnik 44.
[24] See n 22.

2014, which stipulated that SOVA may conduct certain types of surveillance without a court order (such as surveillance of international communication systems and covert surveillance of public spaces), while interception and wiretapping of private correspondence require prior authorisation from the President of the Supreme Court. The study also emphasises the role of the Constitutional Court in limiting data retention obligations and the importance of oversight mechanisms, including the Parliamentary Commission for Supervision of the Intelligence and Security Services, the Information Commissioner, and the Human Rights Ombudsman. Despite these safeguards, the report notes that the law does not explicitly prohibit non-suspicion-based or indiscriminate large-scale surveillance, particularly in the context of international communications, and that certain rights of individuals (such as the right to be informed or to access personal data) may be limited for reasons of national security.

Additional comparative insight is provided by the article The interception of communication in France and Italy – what relevance for the development of English law? (Galli)[25] on the interception of communications in France and Italy, which examines the distinctive features of their interception regimes, recent reforms, and the balance between investigative needs and privacy protections.

Concerning the perspectives outside the EU, an interesting article by Blight on ASIO telecommunications interception and data access powers[26] shows that the Australian Security Intelligence Organisation (ASIO) holds broad powers to intercept telecommunications and access data. The statutory threshold for ASIO to access telecommunications data or intercept telephone services is relatively low, lacking a proportionality test or explicit privacy considerations. Rules around retention, analysis, and dissemination of intercepted data are minimal, and there is no statutory requirement to destroy irrelevant information. These powers are justified by national security imperatives, but have been criticised as outdated in light of technological change and evolving privacy expectations. The Australian regime illustrates a markedly different approach to balancing security and privacy compared to many EU Member States, with less emphasis on judicial oversight and procedural safeguards.

Furthermore, it is interesting to further compare the regulation of telecommunications interception and access with Arab countries, which is addressed in detail in Telecommunications (interception and access) and its Regulation in Arab Countries (Kisswani)[27]. This study highlights that, while telecommunication is essential for modern society, most Arab countries lack comprehensive legislation specifically governing telecommunications interception and access. The absence of such legal frameworks creates challenges for balancing national security, crime investigation, and the protection of individual privacy. The paper also notes that, although some cyber-related laws exist, there is a pressing need for updated and robust regulations to address the realities of modern telecommunication technologies. The Australian legal framework is discussed as a potential model, given its early adoption and ongoing adaptation to technological change. The study further emphasises the importance of aligning interception laws with human rights and privacy standards, and the need for clear procedures, oversight mechanisms, and safeguards to ensure both security and the protection of civil liberties.

[25] Galli F, 'The interception of communication in France and Italy – what relevance for the development of English law?' (2016) 20(5) International Journal of Human Rights 666.
[26] Blight J, 'ASIO telecommunications interception and data access powers' (2023) 48(4) Alternative Law Journal 288.
[27] Kisswani NM, 'Telecommunications (interception and access) and its Regulation in Arab Countries' (2010) 5(4) Journal of International Commercial Law and Technology 225.

Collectively, these comparative and national analyses demonstrate that the landscape of telecommunications interception in criminal investigations remains highly heterogeneous, not only across Europe but globally. The resulting legal and operational complexities underscore the need for ongoing dialogue, harmonisation efforts, and the development of best practices to support effective and rights-compliant cross-border judicial cooperation.

4.1.4 Infrastructural, Technological, Market, and Regulatory Challenges

The technological and regulatory landscape of lawful interception is critically assessed by Doronin (2023)[28], who questions whether lawful interception requirements act as market access barriers within the EU. His analysis reveals how technical standards and regulatory fragmentation can hinder both the deployment of interception technologies and the smooth functioning of the Digital Single Market.

Ventre and Guillot (2023)[29] further explore the technological underpinnings of electronic communication interception, discussing how advancements in interception technologies shift the balance of power between state authorities and private actors. Their work is particularly relevant in the context of encrypted communications and the increasing use of sophisticated tools by law enforcement.

The urgency of harmonising interception regulations for effective law enforcement is articulated by Fadhil (2020)[30], who argues that regulatory divergence not only complicates cross-border cooperation but also undermines the rule of law and procedural fairness.

In the book chapter 'Communication interception technology' Congram, Bell and Lauchs (Policing Transnational Organized Crime and Corruption: Exploring the Role of Communication Interception Technology, 2013) describe the legislative constraints, privacy concerns, and organisational culture barriers, which limit the communication interception technology effectiveness against transnational organised crime and corruption. Case studies, such as those from Hong Kong, demonstrate that, where legal frameworks permit integrated communication interception technology deployment, intelligence derived from intercepts can yield timely operational insights, enhance understanding of criminal networks, and lead directly to significant arrests and seizures.

However, technical aspects of interception are of equal importance. Fitsanakis, in the book chapter 'The Techniques of Communications Interception' (Redesigning Wiretapping, 2020) categorises interception methods by active vs. passive deployment and inline vs. out-of-band capture. Active techniques integrate interception functions within switches or gateways, while passive methods duplicate traffic via high-capacity probes. Recent improvements in filtering data probes and selectively extracting packet headers have reduced the amount of data that law enforcement agencies need to process by half. This makes it possible to intercept large amounts of internet traffic without causing very high costs for equipment or operations.

Parlov et al. (Information Security and the Lawful Interception of Communications through Telecom Service Providers Infrastructure: Advanced Model System Architecture, 2021) propose

[28] Doronin V, 'Lawful interception–A market access barrier in the European Union?' (2023) 51 Computer Law & Security Review.
[29] Ventre D and Guillot P, *Electronic Communication Interception Technologies and Issues of Power* (John Wiley & Sons 2023).
[30] Fadhil M, 'The urgency of the harmonization of interception regulation in the context of law enforcement' (2020) 3(2) Substantive Justice International Journal of Law 125.

an advanced lawful interception architecture for telecom-provider infrastructure that extends ETSI standards to IP-based channels. Their model unifies interception of voice, SMS/MMS, e-mail, VoIP, and rich-communication services through a mediation function embedding robust security controls to ensure data integrity, confidentiality, and availability while preserving subscriber privacy.

4.1.5 Encrypted Communications, Admissibility, and Case Law

A significant recent development in the field is the interception and decryption of encrypted communications, as exemplified by the high-profile EncroChat and Sky ECC cases. Sachoulidou (2024)[31] analyses the CJEU's decision in Staatsanwaltschaft Berlin v. MN (EncroChat)[32], focusing on the cross-border, data-driven nature of police investigations and the complex questions surrounding the admissibility of evidence obtained through such means. This case illustrates the growing importance – and legal ambiguity – of real-time interception and decryption in contemporary criminal justice.

Jerman Blažič and Klobučar (2019)[33] examine whether the evolving EU judicial environment is sufficient to remove barriers to justice in an interconnected society, considering both legal and technical aspects of cross-border evidence collection, including telecommunications interception.

4.1.6 Synthesis and Gaps

The reviewed literature highlights several persistent and interrelated challenges in the field of cross-border judicial cooperation on (real-time) telecommunications interception. A prominent issue is the fragmentation of legal frameworks and the ongoing lack of harmonisation among EU Member States, which complicates the effective and consistent application of interception measures. Technical and operational barriers also remain significant, particularly in relation to the real-time interception of encrypted communications or those transmitted via Virtual Private Networks (VPN), where law enforcement agencies face evolving technological obstacles.

In addition, the literature points to divergent procedural safeguards and varying standards for the admissibility of evidence, which can undermine mutual trust and the smooth exchange of information across jurisdictions. This is further complicated by the enduring tension between the imperatives of law enforcement and the need to uphold privacy and fundamental rights – an issue that is especially acute in the context of mass surveillance and audio-video monitoring in private spaces.

Despite the progress achieved through instruments such as the EIO Directive, scholars and practitioners alike emphasise the need for further harmonisation of legal standards, the development of clearer procedural guidelines, and the establishment of robust safeguards. Such measures are essential not only for facilitating effective cross-border cooperation but also for ensuring that the fundamental rights of individuals are adequately protected in the rapidly evolving landscape of electronic communications and surveillance.

[31] Sachoulidou A, 'The Court of Justice in Staatsanwaltschaft Berlin v MN (EncroChat): From cross-border, data-driven police investigations to evidence admissibility' (2024) 31(4) Maastricht Journal of European and Comparative Law 510.
[32] See Section 9.1 *infra*.
[33] See n, p. 87.

4.2. EU funded projects

Among the numerous EU-funded projects, none simultaneously addresses the interception of telecommunications, cross-border judicial cooperation, and the practical application of the EIO in a comprehensive manner. Nevertheless, various aspects related to these critical issues have been explored in previous research initiatives and projects, providing valuable insights and groundwork that are highly relevant to the INCEPT project.

The core focus of INCEPT is to facilitate and enhance effective cooperation between competent judicial authorities across EU Member States in the execution of telecommunications interception and the exchange of the resulting electronic evidence. This focus responds to the growing need for harmonised judicial practices and improved operational coordination in the face of increasingly complex cross-border criminal investigations involving electronic communications.

To identify relevant EU-funded projects that contribute to this field, an extensive search was conducted using the CORDIS database, complemented by thorough reviews of project websites and their publicly available deliverables. The following section presents a carefully selected overview of EU-funded projects whose results, methodologies, and experiences are particularly significant for the INCEPT project. These projects provide a solid foundation for INCEPT's work, highlighting areas of complementarity and synergy, and offering opportunities for mutual learning and the development of best practices. By building on these prior efforts, INCEPT aims to address existing gaps and contribute to a more coherent and effective framework for judicial cooperation in the interception and use of electronic evidence across Europe.

INSPECTr[34] (Intelligence Network and Secure Platform for Evidence Correlation and Transfer) is an EU-funded Horizon 2020 project designed to develop a shared intelligent platform that integrates big data analytics, machine learning, blockchain, and standardised digital forensics (CASE format) to enhance law enforcement agencies' (LEAs) capabilities in cross-border cybercrime investigations. The project facilitates secure evidence exchange, real-time case linkage, and advanced analysis while embedding privacy and ethics by design, thus addressing both technological and ethical dimensions of digital investigations.

Key achievements of INSPECTr include creating a reference digital forensics domain model and an open-source prototype platform tested iteratively; integrating advanced analytics such as natural language processing for named entity recognition, computer vision for object recognition, and machine learning for cross-case correlation; adopting the CASE format for evidence standardisation and interoperability; establishing a secure network for multi-jurisdictional evidence discovery with strict legal and ethical data-sharing controls; operating LEA Living Labs for real-world feedback and capacity building; and developing semi-automatic OSINT data extraction tools with enhanced methods for data independence and seriality detection.

INSPECTr complements the INCEPT project by providing the essential technological infrastructure for digital evidence management and cross-border collaboration. While INSPECTr focuses on the technical aspects – ensuring that digital investigations are efficient, interoperable, and privacy-conscious – INCEPT concentrates on legal and procedural harmonisation for the admissibility and judicial cooperation of electronic evidence. Together, they form a holistic solution

[34] European Commission, 'Intelligence Network and Secure Platform for Evidence Correlation and Transfer (INSPECTr) – Project results' (CORDIS 2019) https://cordis.europa.eu/project/id/833276/results accessed 31 July 2025.

strengthening Europe's fight against cyber-enabled crime by bridging technology and law, enhancing judicial readiness, and aligning operational ethics and policies[35][36].

SIMARGL[37] (Secure Intelligent Methods for Advanced Recognition of Malware and Stegomalware) was an EU-funded project aimed at improving cybersecurity by developing advanced tools to detect malware that uses hidden communication techniques, such as stegomalware. The project addressed cyber threats that can impact both individuals and critical infrastructures.

Key achievements relevant to INCEPT include:

- Developing a validated toolkit for detecting hidden malware using machine learning and signal processing.
- Providing privacy- and security-by-design solutions compliant with GDPR.
- Training law enforcement agencies (LEAs) on threats posed by information hiding techniques.
- Offering policy recommendations to strengthen EU cybersecurity frameworks.

How INCEPT complements SIMARGL:

- Bridging Technology and Law: SIMARGL delivers the technical means to uncover concealed cyber threats, while INCEPT focuses on the legal and procedural frameworks needed to handle electronic evidence derived from such detection, especially in judicial and cross-border contexts.
- Enhancing Judicial Readiness: INCEPT prepares judicial authorities to interpret and use new types of e-evidence uncovered by technologies like those developed in SIMARGL.
- Policy Synergy: Both projects provide valuable recommendations – SIMARGL from a cybersecurity perspective, INCEPT from a legal cooperation standpoint – together informing comprehensive EU policy.

Together, SIMARGL and INCEPT address both the technical and legal challenges of combating cybercrime and interception of concealed digital communications across Europe[38].

The **RevACLaw**[39] (Revamping Anticorruption Criminal Law – Strategies and Consequences) addresses the challenge of transnational corporate corruption and how criminal justice systems have adapted through evolving substantive and procedural criminal law, including mutual legal assistance frameworks. The project studies a hybrid model of corporate criminal justice, notably the use of non-trial settlements in jurisdictions like France, Switzerland, the UK, and the USA.

Key objectives relevant to INCEPT:

- Analysing strategies reshaping criminal justice in corporate corruption cases.

[35] See n 15.
[36] European Commission, 'D8.8 Guide on privacy and ethics-by-design in law enforcement technology' (28 February 2023) https://inspectr-project.eu/resources/public/INSPECTr_Public_Deliverable_D8.8.pdf accessed 31 July 2025.
[37] European Commission, 'Secure Intelligent Methods for Advanced RecoGnition of malware and stegomalware (SIMARGL) – Project results' (CORDIS 2019) https://cordis.europa.eu/project/id/833042 accessed 31 July 2025.
[38] European Commission, 'Deliverable D 6.3 SIMARGL Full solution release. Integration, Validation and Demonstration' (29 April 2022) https://cordis.europa.eu/project/id/833042/results accessed 31 July 2025.
[39] European Commission, 'Revamping Anticorruption Criminal Law – Strategies and Consequences (RevACLaw) – Project results' (CORDIS 2020) https://cordis.europa.eu/project/id/864498 accessed 31 July 2025.

- Examining transparency and accessibility of non-trial settlements.
- Investigating challenges related to victim participation and prosecutorial discretion.

How INCEPT complements RevACLaw:

- Cross-Border Legal Cooperation: While RevACLaw focuses on corporate crime and settlement practices, INCEPT addresses judicial cooperation and procedural aspects of electronic evidence and interception in multi-jurisdictional investigations.
- Enhancing Judicial Capacity: INCEPT helps judicial authorities handle complex cross-border evidence such as intercepted communications, complementing RevACLaw's insights on complex settlement proceedings.
- Legal Harmonisation: INCEPT promotes clarity and harmonisation in applying EU directives and conventions for interception cases, supporting transparency and legal certainty highlighted as challenges by RevACLaw.
- Protecting Victims and Evidence Integrity: INCEPT's focus on admissibility and proper handling of e-evidence strengthens victims' rights and judicial fairness, addressing gaps identified by RevACLaw.

Together, RevACLaw and INCEPT provide complementary perspectives: RevACLaw offers a conceptual and empirical understanding of evolving criminal justice models in corporate corruption, while INCEPT develops practical tools and legal clarity for judicial cooperation in the interception and use of electronic evidence in cross-border investigations[40].

The **HEROES**[41] (Novel Strategies to Fight Child Sexual Exploitation and Human Trafficking Crimes and Protect their Victims) addresses the increased challenges posed by human trafficking and child sexual abuse crimes, amplified by digital technologies and the COVID-19 pandemic. The project uses an interdisciplinary and victim-centred approach to improve prevention, investigation, and victim support.

Key aspects relevant to INCEPT:

- Developing AI-based and OSINT tools for detecting illegal content and grooming activities.
- Creating training programs for law enforcement, the judiciary, and civil society actors.
- Tackling legal and privacy challenges related to digital forensics and e-evidence, promoting harmonisation across EU and non-EU countries.
- Enhancing information exchange and coordination among stakeholders.

How INCEPT complements HEROES:

- Cross-Border Judicial Cooperation: Both emphasise harmonised legal frameworks and coordinated judicial responses to cross-border crimes.
- Use of E-Evidence: HEROES focuses on challenges in obtaining and using electronic evidence in trafficking and exploitation cases, aligning with INCEPT's work on interception and admissibility of such evidence.

[40] Capus N and Hohl Zuercher F, 'Revamping Anticorruption Criminal Law: The Making of (In-)Transparency. Negotiated Justice in Transnational Corruption – between Transparency and Confidentiality' (2024) 1-32.
[41] European Commission, 'Novel strategies to fight child sexual exploitation and human trafficking crimes (HEROES) – Project results' (CORDIS 2021) https://cordis.europa.eu/project/id/101021801 accessed 31 July 2025.

- Capacity Building: Both projects prioritise training for judicial and law enforcement actors to manage technological and legal complexities.
- Victim Protection: HEROES adopts a victim-centred approach, while INCEPT safeguards fundamental rights in interception and evidence handling, supporting victim protection legally.
- Technology and Legal Frameworks: HEROES advances technological detection tools; INCEPT focuses on legal and procedural frameworks for their lawful judicial use.

Together, HEROES and INCEPT offer a comprehensive EU response combining innovative technology, victim-centred policies, and harmonised judicial cooperation to prevent and prosecute serious cross-border crimes while upholding fundamental rights[42].

The **TRACE**[43] (Tracking Illicit Money Flows) addresses the challenges posed by transnational criminal networks exploiting advanced ICTs to facilitate illicit financial flows (IFFs) and related crimes, including terrorist financing and money laundering via cryptocurrencies. The project develops AI-driven tools and an open-source modular platform to help law enforcement agencies (LEAs) and financial intelligence units trace illicit money trails and analyse cross-border financial flows in real time.

Key features relevant to INCEPT:

- AI-enabled solutions for detecting and tracking illicit financial movements.
- Harmonisation of e-evidence standards and fostering information sharing among EU LEAs.
- Integration of ethics-by-design to ensure compliance with data protection and fundamental rights.
- Collaboration with various stakeholders to co-develop and validate investigative tools.
- Providing recommendations on legal frameworks and best practices for cross-border investigations.

How INCEPT complements TRACE:

- While TRACE develops cutting-edge technological tools for detecting illicit money flows, INCEPT focuses on the legal and procedural aspects of judicial cooperation, particularly interception of telecommunications and admissibility of electronic evidence.
- TRACE primarily supports LEAs and financial intelligence units in operational investigations, whereas INCEPT serves legal practitioners, judges, and prosecutors to ensure lawful and effective use of evidence in courts.
- Both projects emphasise harmonisation of legal standards and ethical compliance to facilitate cross-border cooperation.

[42] European Commission, 'HEROES Deliverable D4.4 Manual for Early Identification of Potential Victims of Trafficking in Human Beings, Child Sexual Abuse and Child Sexual Exploitation' (CORDIS 2023) https://cordis.europa.eu/project/id/101021801/results accessed 2 August 2025.
[43] European Commission, 'Tracking illicit money flows (TRACE) – Project results' (CORDIS 2021) https://cordis.europa.eu/project/id/101022004 accessed 31 July 2025.

Together, TRACE and INCEPT provide a holistic approach by combining technological innovation with strengthened legal frameworks, enhancing Europe's capacity to investigate, prosecute, and prevent complex cross-border criminal activities[44][45].

The **CREST**[46] (Fighting Crime and TerroRism with an IoT-enabled Autonomous Platform) develops an advanced technological platform integrating Internet of Things (IoT), autonomous systems, AI, and blockchain to enhance law enforcement agencies' (LEAs) capabilities in crime and terrorism prevention, detection, and investigation. The platform supports operational tasks such as threat assessment, dynamic mission planning, secure information sharing, and digital evidence exchange with guaranteed chain of custody. CREST's solutions are applied in use cases including protection of public figures, counterterrorism in crowded spaces, and cross-border operations against organised crime.

Key innovations relevant to INCEPT:

- AI-driven threat detection and autonomous mission planning.
- Blockchain-based secure evidence sharing.
- Emphasis on ethics and privacy by design, ensuring compliance with EU and national laws.
- Training and awareness materials to support LEAs operationally.

How INCEPT complements CREST:

- CREST provides cutting-edge technological tools to improve LEAs' operational effectiveness, while INCEPT focuses on the judicial and legal frameworks necessary for admissible and lawful use of intercepted communications and electronic evidence.
- INCEPT enhances judicial cooperation, capacity building, and harmonisation of legal standards among judges, prosecutors, and investigators, ensuring cross-border cooperation mechanisms are aligned with EU directives and regulations such as the European Investigation Order (EIO) and Mutual Legal Assistance Regulation (MLAR).
- Both projects embed ethical and privacy safeguards – CREST through technology design, INCEPT through legal compliance and fundamental rights protection.

Together, CREST and INCEPT offer complementary solutions that improve both the technological capacities of law enforcement and the legal robustness of judicial processes, contributing to an integrated, effective, and rights-compliant European criminal justice system[47].

The **TITANIUM**[48] (Tools for the Investigation of Transactions in Underground Markets) develops advanced forensic tools to help law enforcement agencies (LEAs) investigate criminal and

[44] European Commission, 'TRACE Deliverable D10.11 – TRACE project's final conference' (CORDIS 2021) https://cordis.europa.eu/project/id/101022004/results accessed 2 August 2025.
[45] European Commission, 'TRACE Deliverable D7.4 – Assessment of the scope and efficacy of European cyber forensics and recommendations to improve capacities and policies on detecting illicit money flows' (CORDIS 2021) https://cordis.europa.eu/project/id/101022004/results accessed 2 August 2025.
[46] European Commission, 'Fighting Crime and Terrorism with an IoT-enabled Autonomous Platform (CREST) – Project results' (CORDIS 2019) https://cordis.europa.eu/project/id/833464 accessed 31 July 2025.
[47] European Commission, 'CREST Deliverable D1.4: Public final activity report: WP1 – Project management and coordination' (CORDIS 2019) https://cordis.europa.eu/project/id/833464/results accessed 2 August 2025.
[48] European Commission, 'Tools for the Investigation of Transactions in Underground Markets (TITANIUM) – Project results' (CORDIS 2017) https://cordis.europa.eu/project/id/740558 accessed 31 July 2025.

terrorist activities involving virtual currencies and dark web marketplaces. The project addresses the challenges of anonymity in cryptocurrencies and darknet transactions by providing open-source tools for monitoring, de-anonymisation, and detailed analysis of blockchain data.

Key achievements relevant to INCEPT:

- Creation of a comprehensive forensic toolset including dark web monitors and cryptocurrency analysers.
- Use of machine learning to detect money laundering, tumblers, and suspicious transaction patterns.
- Validation of tools through operational field labs with participation from LEAs.
- Incorporation of legal and ethical compliance to protect privacy and fundamental rights.
- Collaboration with INTERPOL to set global standards on forensic data exchange for darknet investigations.

How INCEPT complements TITANIUM:

- TITANIUM focuses on developing technical capabilities for detecting and analysing digital evidence, while INCEPT addresses judicial cooperation and legal frameworks ensuring admissibility and proper use of such evidence across borders.
- INCEPT supports harmonisation of mutual legal assistance, interception laws, and capacity building for judicial practitioners to effectively use evidence derived from tools like those developed by TITANIUM.
- Both projects prioritise ethical and privacy safeguards aligned with EU fundamental rights and relevant regulations, such as the European Investigation Order (EIO) and Mutual Legal Assistance Regulation (MLAR).

Together, TITANIUM and INCEPT combine innovative investigative technologies with the necessary legal and procedural frameworks to tackle complex cyber-enabled crimes effectively and lawfully within the European criminal justice system[49][50].

The **VICTORIA**[51] (Video Analysis for Investigation of Criminal and Terrorist Activities) develops advanced video analysis tools to support law enforcement agencies (LEAs) in efficiently processing large volumes of video data related to crimes and terrorism. The project created a scalable Video Analysis Platform (VAP) that accelerates video examination by up to 100 times, incorporating big data architecture, semantic queries, 4D crime scene reconstruction, and virtual reality tools.

Key achievements relevant to INCEPT:

- Advanced video and audio analytics integrated into a user-friendly platform tailored to LEA needs.

[49] European Commission, 'D8.1 Project Handbook' (TITANIUM Consortium) https://cordis.europa.eu/project/id/740558/results accessed 23 May 2025.
[50] European Commission, 'TITANIUM Deliverable D3.5 User experience and forensics reporting guidelines' (CORDIS 2017) https://cordis.europa.eu/project/id/740558/results accessed 2 August 2025.
[51] European Commission, 'Video analysis for Investigation of Criminal and Terrorist Activities (VICTORIA) – Project results' (CORDIS 2017) https://cordis.europa.eu/project/id/740754 accessed 31 July 2025.

- Validation in field trials and live investigations, accompanied by extensive training for LEA personnel.
- Compliance with EU legal, ethical, and privacy standards embedded throughout the platform's design.

How INCEPT complements VICTORIA:

- VICTORIA focuses on technological innovation for operational video analysis, while INCEPT addresses the legal and procedural frameworks necessary for the admissibility and cross-border exchange of electronic evidence, including intercepted video recordings.
- INCEPT enhances judicial cooperation, legal harmonisation, and capacity building among judges, prosecutors, and investigators to effectively handle video and other e-evidence within the European legal context, including under the European Investigation Order (EIO) and Mutual Legal Assistance Regulation (MLAR).
- Both projects embed strong ethical and privacy safeguards to protect fundamental rights during evidence processing and judicial cooperation.

Together, VICTORIA and INCEPT provide complementary solutions by combining cutting-edge video investigation technologies with the robust legal and procedural frameworks required for effective and lawful use of such evidence across Europe's criminal justice systems[52][53].

The **EXFILES**[54] (Extract Forensic Information for LEAs from Encrypted SmartPhones) addresses the challenge law enforcement agencies (LEAs) face in extracting digital evidence from modern encrypted smartphones often used in criminal activities. Traditional forensic methods struggle with advanced encryption and security features, delaying investigations.

Key achievements relevant to INCEPT:

- Development of new forensic tools combining software and hardware techniques to lawfully extract data from encrypted devices.
- Advances in reverse engineering mobile Trusted Execution Environments (TEEs), chip deprocessing, and ROM extraction.
- Use of AI to analyse device components and retrieve encryption keys.
- Validation of tools in real-world investigative scenarios.
- Provision of training and guidelines to forensic experts, ensuring ethical and legal compliance.

How INCEPT complements EXFILES**:**

- EXFILES focuses on technological innovation, enabling access to encrypted digital evidence, while INCEPT addresses the judicial cooperation, legal frameworks, and procedural standards required to lawfully obtain, exchange, and admit such evidence in cross-border criminal investigations.

[52] Climente A, 'D8.1 VICTORIA training methodologies and evaluation criteria definition' (VICTORIA Consortium 2017).
[53] Climente A, 'D8.3 VICTORIA training content production and tools selection' (VICTORIA Consortium 2018).
[54] European Commission, 'Extract forensic information for LEAs from encrypted smartphones (EXFILES) – Project results' (CORDIS 2020) https://cordis.europa.eu/project/id/883156 accessed 31 July 2025.

- INCEPT ensures harmonised application of EU directives such as the European Investigation Order (EIO) and Mutual Legal Assistance Regulation (MLAR), fostering capacity building and mutual learning among judicial authorities.
- Both projects prioritise legal and ethical compliance in their respective domains.

Together, EXFILES and INCEPT provide a comprehensive approach: EXFILES empowers LEAs with forensic capabilities to uncover encrypted evidence, and INCEPT establishes the legal and procedural foundation for using that evidence effectively and lawfully, promoting an integrated and rights-respecting European criminal justice system[55].

The **RAMSES**[56] (Internet Forensic Platform for Tracking the Money Flow of Financially-Motivated Malware) develops an intelligent, scalable platform to aid law enforcement agencies (LEAs) in investigating financially motivated malware crimes such as ransomware and banking Trojans. The platform extracts and analyses data from the public and deep web to identify fraudulent patterns and trace malware sources.

Key aspects relevant to INCEPT:

- Utilisation of Big Data technologies for handling large volumes of structured and unstructured forensic data.
- Integration of tools for malware payment tracking, multimedia manipulation detection, and malware sample analysis.
- Validation through mono- and multi-LEA pilots across several European countries.
- Compliance with European ethical, legal, and privacy standards.

How INCEPT complements RAMSES:

- RAMSES focuses on developing advanced forensic technologies to detect and analyse malware-related evidence, while INCEPT addresses the judicial cooperation and legal frameworks essential for the lawful admission and cross-border exchange of such electronic evidence.
- INCEPT promotes harmonisation of procedures and capacity building among judicial authorities in accordance with the European Investigation Order (EIO) and Mutual Legal Assistance Regulation (MLAR).
- Both projects emphasise the protection of fundamental rights and enhancing cross-border collaboration during criminal investigations.

Together, RAMSES and INCEPT provide complementary solutions: RAMSES strengthens LEAs' operational forensic capabilities against cybercrime, while INCEPT ensures the legal and procedural frameworks are in place for effective and rights-compliant judicial use of digital evidence across Europe[5758].

All legal proceedings depend on evidence, and electronic evidence must be shown to be unaltered from the time it was obtained. Due to the ease of manipulating digital data, maintaining

[55] Dequesnes A, Baudouin L, Debruyne C, Lanux T, Leleu S, Moritz M, Serap S and EXFILES Consortium, 'D2.1 Fundamental support study on encryption and fundamental rights' (Université Lille 2022).
[56] European Commission, 'Internet Forensic platform for tracking the money flow of financially-motivated malware (RAMSES) – Project results' (CORDIS 2016) https://cordis.europa.eu/project/id/700326 accessed 31 July 2025.
[57] European Commission, 'RAMSES D8.2 training material and plan of training sessions for law enforcement agents' (CORDIS 2018).
[58] BayFHVR, 'D9.5 Dissemination materials and final report' (Deliverable D9.5, H2020 Project RAMSES, Grant No 700326, RAMSES Consortium 2019).

and proving its integrity is crucial. However, many European criminal procedure laws predate digital technologies, resulting in inconsistent regulations and difficulties in cross-border evidence exchange. The **EVIDENCE**[59] (European Informatics Data Exchange Framework for Courts and Evidence) project aims to create a Common European Framework by providing guidelines, recommendations, and technical standards for the collection, use, and exchange of electronic evidence. This framework will help policymakers, law enforcement, judges, and legal practitioners harmonise practices and improve cooperation across EU Member States. EVIDENCE also fosters a network of digital forensic experts and has developed tools and proposals to standardise electronic evidence handling. The project collaborates with initiatives like e-Codex to pilot secure evidence exchange aligned with EU legal instruments, ultimately supporting faster and more efficient cross-border criminal investigations[60] [61].

INCEPT builds directly on the groundwork laid by EVIDENCE, moving from the development of strategic frameworks to their practical implementation in real judicial contexts. While EVIDENCE focused on identifying gaps and proposing harmonised solutions, INCEPT operationalises these recommendations by training judges, prosecutors, and investigators, and by fostering mutual learning and capacity building. INCEPT ensures that the legal and procedural standards envisioned by EVIDENCE are effectively adopted in daily practice, particularly under the European Investigation Order and Mutual Legal Assistance Regulation. In this way, INCEPT complements EVIDENCE by translating its roadmap into tangible improvements in judicial cooperation, legal certainty, and the lawful, rights-respecting use of electronic evidence across Europe. Together, the two projects form a continuum from conceptualisation to implementation, driving the evolution of a robust, integrated European framework for digital evidence.

FORMOBILE[62] (From mobile phones to court – A complete FORensic investigation chain targeting MOBILE devices) is a European project dedicated to establishing a comprehensive end-to-end forensic investigation chain specifically for mobile devices, recognising the central role that smartphones and other mobile technologies play in modern criminal activities. The project addresses the technical, legal, and procedural challenges law enforcement faces in recovering, decoding, and analysing data from mobile phones, such as call logs, messages, browser histories, and GPS locations. FORMOBILE developed new tools to unlock and extract previously inaccessible data, created a European standard (CEN Workshop Agreement 17865) for mobile forensics, and delivered a structured training curriculum for police and forensic practitioners. The project also emphasised legal and ethical compliance, ensuring all solutions respect GDPR and criminal procedure rules, and it engaged a broad network of stakeholders through dissemination and capacity-building activities. FORMOBILE's achievements include innovative RAM acquisition tools, cloud extraction solutions, advanced data analysis platforms, and a harmonised approach to mobile forensic investigations, all aimed at enhancing the quality, speed, and reliability of digital evidence in criminal proceedings.

[59] European Commission, 'European Informatics Data Exchange Framework for Courts and Evidence (EVIDENCE) – Project results' (CORDIS 2014) https://cordis.europa.eu/project/id/608185 accessed 31 July 2025.
[60] European Commission, 'European Informatics Data Exchange Framework for Courts and Evidence (EVIDENCE) – Project results' (CORDIS 2014) https://cordis.europa.eu/project/id/608185 accessed 31 July 2025.
[61] European Informatics Data Exchange Framework for Courts and Evidence project, 'Deliverable D4.1' http://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d4-1-413.pdf accessed 31 July 2025.
[62] European Commission, 'From mobile phones to court – A complete FORensic investigation chain targeting MOBILE devices (FORMOBILE) – Project results' (CORDIS 2019) https://cordis.europa.eu/project/id/832800 accessed 31 July 2025.

Compared to INCEPT, which focuses on harmonising legal frameworks, building capacity, and fostering mutual learning for the cross-border exchange and admissibility of electronic evidence under instruments like the European Investigation Order (EIO) and Mutual Legal Assistance Regulation (MLAR), FORMOBILE is more technically oriented and specialised in the domain of mobile forensics. While INCEPT addresses the broader judicial cooperation and procedural mechanisms necessary for the lawful use and exchange of all forms of electronic evidence, FORMOBILE concentrates on developing operational standards, tools, and training specifically for mobile device investigations. The two projects are complementary: FORMOBILE strengthens the technical and procedural capabilities for mobile evidence acquisition and analysis, while INCEPT ensures that such evidence can be effectively and lawfully used in cross-border judicial contexts, bridging the gap between technical innovation and legal harmonisation in the European justice system[63].

The project 'Improving the Application of the Presumption of Innocence in the Use of Electronic Evidence (**INNOCENT**)' focuses on the procedural rights of individuals suspected or accused of criminal offences, particularly their right to presumption of innocence until proven guilty, and how this could be interpreted in the context of electronic evidence. INNOCENT exclusively targets jurisdictions in Central and Eastern Europe to map similarities, best practices, and challenges in the region regarding the practical application of the presumption of innocence. Furthermore, INNOCENT aims to strengthen cooperation among neighbouring jurisdictions concerning the intersection between the presumption of innocence and electronic evidence.

INNOCENT's main achievements include:
The development of a comprehensive Toolkit for handling and admissibility of electronic evidence: empowering legal practitioners to critically review electronic evidence from the procedural rights perspective, written by Prof Dr Benjamin Flander and Prof Dr Anže Erbežnik, which significantly advances the application of the presumption of innocence in cases involving electronic evidence (e-evidence) in criminal proceedings. It empowers legal practitioners – particularly judges, prosecutors, and defence lawyers in Central and Eastern Europe – to critically assess e-evidence from a procedural rights perspective. Covering the entire 'life cycle' of e-evidence, the Toolkit addresses legal and practical challenges related to the acquisition, admissibility, and cross-border exchange of data stored on electronic devices and in online systems. While it provides guidance on data held by individuals and service providers, it deliberately excludes issues related to the interception of real-time communications, mass surveillance, and predictive policing strategies, maintaining a focused approach on procedural fairness in criminal justice[64].

EUROCOORD[65] (Best Practices for EUROpean COORDination on investigative measures and evidence gathering) is a European project aimed at enhancing judicial cooperation by conducting systematic research and developing specific knowledge and tools to support the effective and coherent application of Directive 2014/41/EU on the European Investigation Order (EIO) in criminal matters, along with other relevant regulations. Its objectives include generating insights

[63] Hummert C and Pawlaszczyk D, *Mobile Forensics – The File Format Handbook: Common File Formats and File Systems Used in Mobile Devices* (Springer 2022).
[64] Flander B and Erbežnik A, 'Toolkit for Handling and Admissibility of Electronic Evidence: Empowering Legal Practitioners to Critically Review E-Evidence from the Procedural Rights Perspective' https://www.zrs-kp.si/wp-content/uploads/2024/07/INNOCENT_monografija_online_edition.pdf accessed 31 July 2025.
[65] European Commission, 'Project details: 723198' (EU Funding & Tenders Portal 2025) https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/projects-details/31070247/723198 accessed 31 July 2025.

to optimise EIO implementation, particularly regarding evidence transmission and admissibility, equipping stakeholders with necessary competencies and protocols to facilitate cross-border cooperation, and raising awareness through dissemination and training activities. The project involves extensive engagement with prosecutors, judges, law enforcement officers, defence lawyers, NGOs, and accused individuals, producing research reports, a Code of Best Practices for EIO, training materials, and establishing a European Observatory on EIO to foster open debate and continuous assessment.

Compared to INCEPT, which focuses on harmonising legal frameworks and building judicial capacity specifically around interception of telecommunications and electronic evidence admissibility under instruments like the EIO and Mutual Legal Assistance Regulation (MLAR), EUROCOORD has a broader remit centred on the overall application and optimisation of the EIO across criminal proceedings. While EUROCOORD emphasises research, best practice development, and stakeholder training to improve procedural coherence and evidence handling across jurisdictions, INCEPT operationalises these frameworks by providing practical tools, training, and legal clarity to judicial actors handling complex electronic evidence, including interception data, in cross-border cases. Together, EUROCOORD and INCEPT complement each other by combining strategic research and policy development with practical implementation and capacity building, thereby strengthening the efficiency, transparency, and legal certainty of European judicial cooperation in criminal matters[66].

4.3. Other projects

While INCEPT builds extensively on the foundation laid by numerous EU-funded projects, it is important to recognise that related themes – such as interception of telecommunications, cross-border judicial cooperation, and the legal handling of electronic evidence – have also been the focus of important initiatives outside the European Union. These non-EU projects and programs, often supported by international organisations, national agencies, or global research consortia, address comparable challenges and offer complementary perspectives that enrich the context in which INCEPT operates.

The core mission of INCEPT remains centred on facilitating and strengthening cooperation among judicial authorities within the EU to harmonise practices in telecommunications interception and the exchange of electronic evidence. However, the complex and transnational nature of cyber-enabled crimes demands a broader understanding of global trends, legal frameworks, technological solutions, and operational models developed beyond the EU borders.

To this end, a systematic review of relevant international projects, initiatives, and policy programs was conducted by exploring global research databases, international law enforcement collaborations, and multilateral frameworks focused on cybersecurity, digital forensics, and judicial cooperation. The following section provides an overview of selected non-EU projects and programs whose results, methodologies, and experiences hold particular relevance for INCEPT. By integrating these international insights, INCEPT is better positioned to foster innovation, promote legal harmonisation, and build robust networks that transcend regional boundaries –

[66] European Commission, 'D3.3 Best practices for EUROpean COORDination on investigative measures and evidence gathering' (15 January 2019) https://www3.ubu.es/eurocoord/wp-content/uploads/2019/06/D3.3-NATIONAL-REPORTS-ON-EIO_rev.pdf accessed 31 July 2025.

thereby contributing to more effective and rights-compliant judicial cooperation in the interception and use of electronic evidence worldwide.

Eurojust Digital Criminal Justice (DCJ) Programme[67] is a transformative initiative designed to modernise and streamline cross-border judicial cooperation within and beyond the EU. By focusing on the digitalisation of criminal justice systems, the programme delivers secure and interoperable digital platforms that enable judicial authorities to communicate, exchange evidence, and coordinate investigations efficiently and securely.

Key elements:

- Deployment of secure, encrypted e-communication infrastructure to protect sensitive data and facilitate real-time collaboration among prosecutors and judges.
- Implementation of standardised digital tools and interoperability frameworks for seamless cross-border cooperation, enabling effective management of electronic evidence in large, complex cases.
- Support for case management, document exchange, and procedural harmonisation to overcome the diverse IT and legal environments in different countries.

INCEPT stands to benefit from the technological backbone established by the DCJ Programme, particularly its secure communication channels and data management platforms. While the DCJ's focus is on infrastructural and operational aspects, INCEPT adds value by developing harmonised legal procedures, capacity-building activities, and specific guidelines for the admissibility of electronically intercepted evidence. Together, they enable a truly interconnected and judicially robust environment for cross-border investigations.

INTERPOL's Project Leader[6869] (Digital Forensics Capacity Building) Initiative is a flagship capacity-building effort aimed at strengthening the digital forensic abilities of law enforcement agencies, especially in Asia and partner countries beyond the EU. The project delivers specialised training, develops guidelines, and supports SOPs in digital forensics to bolster the investigation and prosecution of cybercrime.

Key elements:

- Organisation of comprehensive workshops and hands-on training sessions covering digital forensics, evidence preservation, chain of custody, and forensic readiness.
- Development and dissemination of best practice guidelines and standard operating procedures for digital evidence analysis and management.
- Promotion of international judicial cooperation via knowledge exchange forums and operational coordination among diverse law enforcement bodies.

While INTERPOL Project Leader addresses the critical skills gap in digital forensics at the investigative level, INCEPT complements this by targeting judicial authorities (prosecutors, judges) and ensuring that forensic methods comply with legal and procedural standards necessary for evidence admissibility in court. By harmonising standards and building capacity on

[67] Eurojust, 'Digital Criminal Justice Programme' (European Union Agency for Criminal Justice Cooperation 2025) https://www.eurojust.europa.eu/judicial-cooperation/instruments/digital-criminal-justice-programme accessed 31 July 2025.
[68] INTERPOL, 'Project Leader' (2023) https://www.interpol.int/en/How-we-work/Innovation/Projects/Project-Leader accessed 31 July 2025.
[69] INTERPOL, 'Digital forensics: Helping our member countries make best use of electronic evidence' (2024) https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics accessed 31 July 2025.

both the law enforcement and judicial sides, the two initiatives support the holistic handling of electronic evidence in cross-border crime.

CyberEast+[70] (Council of Europe and EU) is a large-scale partnership between the Council of Europe and the European Union, focused on bolstering cybercrime policies and electronic evidence legislation in Eastern Partnership countries, including Armenia, Azerbaijan, Belarus, Georgia, Moldova, and Ukraine.

Key elements:

- Support for the implementation of the Budapest Convention on Cybercrime and related standards in domestic legal systems.
- Facilitation of legislative alignment, capacity building, and institution-strengthening actions to enable effective cybercrime investigations and e-evidence handling.
- Organisation of regional workshops, technical assistance, and peer-to-peer learning among Eastern Partnership countries and EU Member States.

CyberEast+ extends cross-border cooperation frameworks beyond the EU, focusing on legal harmonisation and operational readiness for cybercrime investigations and electronic evidence management. INCEPT builds on this by providing specialised instruments and training for the EU context, particularly regarding interception of telecommunications and application of the European Investigation Order (EIO). Both projects foster mutual recognition of procedural standards and promote a seamless approach to transnational cybercrime.

The **UNDERSERVED**[71] project is primarily dedicated to addressing the cybersecurity needs of sectors that often operate outside the focus of traditional critical infrastructure frameworks. These sectors – such as humanitarian organisations and various non-profits – face unique challenges related to cybersecurity funding and expertise. UNDERSERVED seeks to bridge this gap by developing a specialised cyber threat reporting and analysis platform that empowers these organisations to report incidents efficiently and effectively to law enforcement agencies. This enhanced reporting capability not only improves the timeliness and accuracy of cyber incident detection but also facilitates the sharing of threat intelligence across jurisdictions, which is critical in today's interconnected digital landscape. By bringing these often-overlooked sectors into the fold of cyber threat cooperation, UNDERSERVED helps create a more comprehensive picture of the cybersecurity environment, allowing law enforcement agencies to respond more effectively to emerging threats.

FREETOOL[72], on the other hand, focuses on empowering law enforcement agencies worldwide by providing free, open-source digital forensic tools designed to improve the analysis and handling of digital evidence. Recognising that many investigative bodies lack the financial resources to acquire expensive forensic software and training, FREETOOL offers accessible technological solutions coupled with educational resources to raise the overall forensic capacity of these agencies. By fostering standardised practices in digital evidence collection, preservation, and analysis, FREETOOL ensures that law enforcement bodies can produce reliable and legally

[70] Council of Europe, 'CyberEast+' (Cybercrime Programme Office 2025) https://www.coe.int/en/web/cybercrime/cybereast-en accessed 31 July 2025.
[71] University College Dublin Centre for Cybersecurity and Cybercrime Investigation, 'UNDERSERVED Cyber Threat Reporting Platform' https://www.ucd.ie/cci/projects/underserved/ accessed 31 July 2025.
[72] University College Dublin Centre for Cybersecurity and Cybercrime Investigation, 'FREETOOL' https://www.ucd.ie/cci/projects/freetool/ accessed 31 July 2025.

admissible evidence. The project's emphasis on practical training and best practices also helps build sustainable expertise among investigators, which is critical when dealing with complex forms of electronic evidence such as intercepted telecommunications.

Together, these projects form a complementary pair that addresses distinct yet interconnected aspects of cybercrime investigation. Whereas UNDERSERVED strengthens the front line by improving incident reporting and intelligence sharing from vulnerable sectors, FREETOOL bolsters the downstream investigative processes by enhancing forensic capabilities and evidence handling. This comprehensive approach fills crucial gaps in the fight against cybercrime by covering both the detection and the judicial processing of digital evidence.

The relevance of UNDERSERVED and FREETOOL to the INCEPT project is substantial. INCEPT's mission is to improve judicial cooperation and procedural harmonisation in cases involving the interception of telecommunications and electronic evidence, tasks that require well-coordinated efforts among prosecutors, judges, and law enforcement officers. The capacity-building components of both UNDERSERVED and FREETOOL align closely with INCEPT's goals by providing accessible and practical tools and training that support the effective handling of intercepted telecommunications data. Moreover, the harmonisation of forensic methodologies promoted by FREETOOL complements INCEPT's efforts to standardise the admissibility and judicial review of electronic evidence across different jurisdictions. The incident reporting platform developed by UNDERSERVED enhances cross-border investigative cooperation by ensuring that law enforcement receives timely and accurate information from a wider array of sectors, ultimately facilitating better mutual assistance under frameworks like the European Investigation Order.

In essence, UNDERSERVED and FREETOOL contribute vital technical and procedural foundations that enable INCEPT to advance its aim of seamless judicial cooperation in the digital age. They help bridge both technological and institutional divides, ensuring that evidence derived from telecommunications interception is both reliable and admissible, while fostering enhanced collaboration across borders. This synergy is particularly important given the complexity of modern cybercrime and the diverse range of actors involved in its detection and prosecution. Together, these projects embody a holistic approach to strengthening the justice system's capacity to respond effectively to intercepted electronic evidence in an interconnected world.

These international projects and programs advance critical dimensions of cross-border judicial cooperation, digital forensics, and the legal handling of electronic evidence. INCEPT complements and builds upon these efforts by focusing on harmonised judicial procedures, capacity building, and the operational application of legal frameworks specifically for intercepted communications and electronic evidence, reinforcing a robust and interoperable European and global justice system.

5. EUROPEAN UNION FRAMEWORK

While lawful interception of telecommunications in criminal proceedings is primarily a national competence, it is regulated indirectly at the EU level through legal instruments on the protection of fundamental rights in criminal proceedings, data protection, telecommunications regulation, and cross-border cooperation in criminal matters.

The core legal instruments include the **Charter of Fundamental Rights of the European Union**,[73] the **Convention on Mutual Assistance in Criminal Matters between the EU Member States**,[74] and **Directive 2014/41/EU on the European Investigation Order**.[75] Another relevant document related to the interception of telecommunications, though not legally binding, is the **Council Resolution on the lawful interception of telecommunications.**[76]

Before the adoption of Directive 2014/41/EU, mutual legal assistance between EU Member States in cross-border access to evidence in criminal matters was also governed by *Council Framework Decision 2008/978/JHA on the European Evidence Warrant,* which aimed to obtain objects, documents, and data for use in criminal proceedings.

In addition to the above-mentioned instruments, several other EU legal acts and documents are also indirectly relevant to the cross-border interception of telecommunications. These include the *EU directives on procedural rights,* the *EU ePrivacy Directive (2002/58/EC),* the *General Data Protection Regulation* (GDPR) (Regulation 2016/679), the *Law Enforcement Directive (Directive 2016/680),* and the *Convention Implementing the Schengen Agreement (CISA).*

Recently, the European Commission presented a **Roadmap for lawful and effective access to data for law enforcement,**[77] a deliverable under the European Internal Security Strategy ('ProtectEU'),[78] which focuses, among other aspects, on obtaining evidence across systems with the lawful interception of telecommunications.

Since 2014, the *EIO Directive provides the main mechanism for judicial cooperation on interception across borders*, however, this area is further shaped by case law from both the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR), emphasising the need for proportionality, necessity, and strong procedural safeguards when intercepting EU citizens' and other individuals' telecommunications.

In this section, we will briefly present four of the aforementioned legal instruments and documents: the Convention, the Directive, the Council Resolution, and the Roadmap.

[73] Charter of Fundamental Rights of the European Union OJ C364/1.
[74] Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union OJ C197/3.
[75] See n 3.
[76] Council Resolution on the lawful interception of telecommunications OJ C329/1.
[77] European Commission, 'Roadmap: Effective and Lawful Access of Law Enforcement Authorities to Electronic Data' (24 June 2025) https://home-affairs.ec.europa.eu/news/commission-presents-roadmap-effective-and-lawful-access-data-law-enforcement-2025-06-24_en accessed 3 August 2025.
[78] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy COM(2025)148 final (1 April 2025) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0148 accessed 4 August 2025.

5.1. Council Resolution on the lawful interception of telecommunications

The Council Resolution on the lawful interception of telecommunications is *a non-binding instrument adopted by the European Union in the context of law enforcement cooperation*, especially during the pre-Lisbon period when the EU's third pillar (Justice and Home Affairs) governed criminal justice and policing matters.

This resolution **facilitates cooperation between law enforcement agencies (LEAs) and telecommunications operators and service providers**, particularly in response to the challenges posed by emerging digital technologies and cross-border communications. It *aims to encourage Member States to implement compatible technical standards and ensure that LEAs in the EU Member States could lawfully intercept telecommunications*, including voice, fax, and digital data, and to harmonise technical standards across the EU to enable effective cooperation.[79]

The resolution opens with a preamble, i.e. a series of recitals that explain the *background, motivation, and objectives of the documen*t. Key themes in the preamble include:

- The need for effective lawful interception capabilities for law enforcement.
- The challenges posed by new telecommunications technologies.
- The importance of technical compatibility across national systems.
- Acknowledgment of fundamental rights and privacy protections.

The main text presents the *'Requirements' for law enforcement agencies relating to the lawful interception of telecommunications*. Terms are defined in the attached glossary.[80]

The resolution urges the Member States to *ensure that telecom operators implement technical capabilities that allow for the lawful interception of communications*, regardless of the technology (e.g., fixed-line, mobile, satellite). It *encourages standardised interception interfaces to allow LEAs to access communications data in a consistent manner across the EU*, while acknowledging the need to balance effective law enforcement with respect for privacy and fundamental rights. An emphasis is also on *ensuring that any interception complies with national legal frameworks*, particularly regarding authorisation procedures, oversight, and privacy safeguards.[81]

The resolution helped pave the way for further international coordination on interception capabilities by informing the development of the so-called 'International User Requirements' for lawful interception adopted jointly by the EU, the United States, Canada, Australia, and others. Despite these developments, *some aspects of the resolution were criticised by privacy advocates as lacking transparency and democratic oversight*.[82]

While the resolution is now obsolete as a policy driver (since 1995, telecommunications technology has evolved significantly and the *resolution's technical assumptions are largely outdated*), it is **historically significant for being one of the** first coordinated EU-level statements **on lawful interception**. It is also considered a *precursor to later instruments, including the EIO Directive*. The resolution also *inspired Member states' national legislation*

[79] See n 76.
[80] *Ibid*.
[81] *Ibid*.
[82] *Ibid*.

implementing modern interception and surveillance laws under data protection and criminal procedure frameworks.

5.2. Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union

Adopted in May 2000 under the former third pillar of the EU (Justice and Home Affairs), the EU MLA Convention is a *foundational legal instrument in the EU's judicial cooperation in criminal matters*. It aims to enhance and modernise mutual legal assistance (MLA) among EU Member States by:

- Improving the speed and efficiency of cooperation.
- Supplementing and, in some cases, going beyond the 1959 Council of Europe European Convention on Mutual Assistance in Criminal Matters.
- Facilitating direct communication between judicial authorities.
- Covering modern investigative techniques, including telecommunications interception, controlled deliveries, and joint investigation teams.[83]

The Convention is structured into several Titles and Articles. Contained in Title III (Articles 17-20), *provisions on 'Interception of Telecommunications' reflect the growing importance of cross-border surveillance in criminal investigations at the turn of the 21st century*. These provisions were groundbreaking at the time, as they established a legal basis for cross-border interception within the EU, addressing legal and technical complexities.

Article 17 – Authorities competent to order interception of telecommunications stipulates that for the purpose of the application of other articles, *'competent authority' shall mean a judicial authority, or, where judicial authorities have no competence in the area covered by those provisions, an equivalent competent authority*.

Article 18 – Requests for interception of telecommunications apply when one Member State requests another to assist with the interception of telecommunications being carried out within the territory of the assisting Member State. This is effectively an *interception with technical assistance from the notified state*. The assisting Member State is asked to intercept, record, or transmit the content of the communications. The request must be made using a standardised form (Annex A) and must include: (1) the authority making the request; (2) the purpose of the interception; (3) the identity of the person or connection to be intercepted; and (4) the technical details necessary to carry it out. The executing Member State must assess legality under its own laws and, if lawful, carry out the request.

Article 19 – Interceptions of telecommunications on national territory by the use of service providers addresses *situations where a Member State intercepts telecommunications that are being transmitted to or from a person in another Member State, but the intercepting State does not need technical assistance from the other State*. The intercepting State must notify the other Member State 'without delay' if the target of the interception is located in that Member State. Notification must include: (1) the legal basis for the interception; (2) the nature of the interception; and (3) information on the authority carrying it out.

The notified Member State can: (a) *object to the interception if it considers it unlawful under its own law*, and (b) *request that interception be terminated or that the information not be used*. This

[83] See n 2, Art. 1.

reflects sovereignty concerns, allowing Member States to retain control over surveillance affecting their territory or residents.

Article 20 – Interception of Telecommunications Without the Involvement of the Target's Member State covers *technical situations where a Member State intercepts telecommunications directly* (*e.g., mobile/satellite communications) without the target being in the intercepting State, without notifying the target's State and without using infrastructure*. This provision is largely technical, but it acknowledges that technological developments (like satellite or mobile routing) may allow for direct interception across borders.

Annex A – Standard Form for Notification or Request provides a *uniform template for both interception with and without assistance*. It shall help ensure consistency, clarity, and legal transparency between Member States.

At the time of its adoption, the Convention was *one of the first legal instruments in Europe to explicitly regulate cross-border telecommunications interception*. It recognised that modern telecommunications (e.g., mobile phones, satellite communication) often cross national borders invisibly. It *included notification and consent mechanisms to protect national sovereignty and privacy rights*.

While the Convention was an advanced legal instrument, *its implementation faced several challenges*, including technical complexity (particularly when routing was unclear or infrastructure was dispersed), divergent national laws (with varying definitions of 'lawful interception' and differing safeguards, making harmonisation difficult), and reservations (as some Member States entered declarations or reservations limiting the scope and application of these provisions).

The Convention entered into force in 2005 after ratification by all then-EU Member States. Following its introduction in May 2017, *it has been partially superseded by the EIO Directive (2014/41/EU), which introduced a new single regime for evidence gathering across borders*.

5.3 Directive 2014/41/EU on the European Investigation Order

5.3.1 The European Investigation Order and the scope of the EIO Directive

Adopted on 3 April 2014, Directive 2014/41/EU on the European Investigation Order (EIO Directive) is **a major EU legal instrument that streamlines and strengthens cross-border evidence gathering in criminal cases across EU Member States**. It *aims to improve efficiency, legal certainty, and mutual trust in judicial cooperation by partially replacing the patchwork of earlier mutual legal assistance instruments*.[84]

The EIO Directive establishes a single, comprehensive framework for the collection and transfer of evidence (except for Joint Investigation Teams) in criminal matters between EU Member States. The investigative measures include, for instance, the hearing of witnesses, communications interceptions, covert investigations and information on banking operations. Unlike earlier judicial cooperation instruments based on mutual legal assistance, which allowed broad possibilities for refusal, the EIO is founded on the ***principle of mutual recognition*** –

[84] Including the Council Framework Decision 2008/978/JHA on the European evidence warrant OJ L350/72, the Council Framework Decision 2003/577/JHA on the execution in the European Union of orders freezing property or evidence OJ L196/45, and the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union OJ C197/3.

meaning that *judicial decisions issued in one Member State must be recognised and executed by another, with only limited grounds for refusal*.

5.3.2 The structure and content of the EIO Directive

The Directive consists of 50 Recitals and 39 Articles, grouped into the following chapters:

Chapter I – The European Investigation Order introduces the concept of the EIO as a *judicial decision* issued or validated by a competent authority in one Member State to have investigative measures carried out in another. An EIO can be issued by a judge, a court, an investigating judge, a public prosecutor competent in the case concerned or any other competent authority (such as law enforcement agencies) as defined by the issuing State (in the latter case, before it is transmitted to the executing authority, the EIO shall be validated by a judge, a court, an investigating judge or a public prosecutor). The EIO applies to criminal proceedings, as well as certain administrative proceedings that can result in penalties. It covers any investigative measure except for the setting up of a joint investigation team. It may also be issued for obtaining evidence that is already in the possession of the competent authorities of the executing State. The issuing of an EIO may also be requested by a suspected or accused person, or by a lawyer on their behalf.

Chapter II and **Chapter III** lay out the **procedures and safeguards for issuing and executing an EIO**. These chapters provide rules on: (a) conditions for issuing and transmitting an EIO; (b) transmission of the EIO; (c) supplement EIO; (d) recognition and execution of the EIO; (e) recourse to a different type of investigative measure; (f) grounds for refusal (e.g., grounds for non-recognition or non-execution); (g) deadlines for recognition or execution; and (d) transfer of evidence; (e) legal remedies available to the suspect; (h) grounds for postponement of recognition or execution; (i) obligation to inform; (j) criminal and civil liability regarding officials; (k) confidentiality; (l) protection of personal data; and (m) costs.

The **issuing authority** may only issue an EIO where: (a) *the issuing of the EIO is necessary and proportionate considering the rights of the suspected or accused person*; and (b) *the investigative measure(s) indicated in the EIO could have been ordered under the same conditions in a similar domestic case*. These conditions ***shall be assessed by the issuing authority in each case***. Where the executing authority has reason to believe that the conditions referred to above have not been met, it may consult the issuing authority and after that consultation the issuing authority may decide to withdraw the EIO.[85]

The **executing authority** *shall recognise an EIO, transmitted in accordance with this Directive, without any further formality being required*. It *shall ensure its execution in the same way as if the investigative measure concerned had been ordered by its own authority*, ***unless that authority decides to invoke one of the grounds for non-recognition or non-execution*** or one of the grounds for postponement provided for in the Directive. *Recognition or execution of an EIO may, among other, be refused in the executing State where*: (a) there is an immunity or a privilege; (b) the execution of the EIO would harm essential national security interests; (c) it would be contrary to the principle of *ne bis in idem*; (d) the EIO has been issued for the offence that is not an offence in the executing State; (e) incompatible with the executing State's obligations to respect fundamental rights; (f) the conduct for which the EIO has been issued does not constitute an

[85] See n 3, Art. 6.

offence under the law of the executing State; and (g) the use of the investigative measure is restricted under the law of the executing State to a list or category of offences which does not include the offence covered by the EIO. Additionally, the executing authority shall have, wherever possible, *recourse to an investigative measure other than that provided for in the EIO.*[86]

The executing authority shall take the decision on the recognition or execution of the EIO as soon as possible and *no later than 30 days after the receipt of the EIO*. It shall carry out the investigative measure without delay and *not later than 90 days following the taking of the decision on the recognition*.[87]

Member States *shall ensure that legal remedies equivalent to those available in a similar domestic case, are applicable to the investigative measures indicated in the EIO*.[88]

Chapter IV – Specific Provisions for Certain Investigative Measures covers common forms of evidence-gathering, including temporary transfer of persons in custody, hearing of witnesses and experts by video or telephone, obtaining of information (bank records, telecoms data, etc.), controlled deliveries, and undercover investigations.

Specific provisions on the **interception of telecommunications** are enshrined in a separate **Chapter V.**

Provisional measures are provided in **Chapter VI.**

The Directive concludes with **Chapter VII – Final provisions.**

The EIO must be issued using a standard form (**Annex A**), containing all essential details for issuing, executing, and validating the EIO. The authority of the executing State which received the EIO must complete the standard form set out in **Annex B**. Another standard form (**Annex C**) is used to notify a Member State about the interception of telecommunication that will be, is or has been carried out on its territory without its technical assistance.

5.3.3 Specific provisions on the interception of telecommunications

Chapter V on the specific legal framework for the interception of telecommunications in cross-border criminal investigations comprises Articles 30 and 31. These articles replace similar provisions in the 2000 EU MLA Convention, but only between states applying the EIO Directive.

Article 30 – Interception of Telecommunications with Technical Assistance applies when the issuing Member State (the one conducting the investigation) needs technical assistance from another Member State (the executing state) to carry out telecommunications interception.

According to this article, an EIO shall contain the information on: (a) the *identification of the subject of the interception;* (b) *the desired duration of the interception*; and (c) the *relevant technical data*. The issuing authority shall *indicate the reasons why it considers the indicated investigative measure relevant for the purpose of the criminal proceedings concerned*.

In addition to the general grounds for refusal, the execution of an EIO related to telecommunications interception ***may also be refused where it would not have been***

[86] *Ibid*., Arts. 9-11.
[87] *Ibid*., Art. 12.
[88] *Ibid*., Art. 14.

authorised in a similar domestic case. The executing State may make its consent subject to any conditions which would be observed in a similar domestic case.

The issuing authority and the executing authority *shall consult each other with a view to agreeing on whether the intercepted data on telecommunications be transmitted to the issuing State immediately or subsequently*.

Subject to the agreement of the executing authority, *an EIO may also include a request for the transcription, decoding, or decryption of the recording*. Any resulting costs shall be borne by the issuing State.

Article 31 – Notification of the Member State where the subject of the interception is located from which no technical assistance is needed applies when a Member State intercepts telecommunications on its own, without needing help from another Member State, but the person being intercepted is located in that other Member State (e.g., if a person in Country B is communicating via satellite or internet-based communication that can be intercepted remotely by Country A without using infrastructure in Country B).

The Article sets out the circumstances in which the intercepting Member State must notify the competent authority of the notified Member State, either before or after the interception takes place.

The notification shall be made by *using the form set out in Annex C*.

The competent authority of the notified Member States may, ***in case where the interception would not be authorised in a similar domestic case***, notify, without delay and at the latest within 96 hours after the receipt of the notification, the competent authority of the intercepting Member State:

(a) that the *interception may not be carried out or shall be terminated*; and
(b) that *any material already intercepted may not be used or may only be used under conditions which it shall specify*.

The competent authority of the notified Member State shall *inform the competent authority of the intercepting Member State of reasons justifying those conditions*.

Since its introduction in May 2017, the EIO mechanism has *provided judicial authorities with a simpler and faster alternative to traditional instruments for requesting evidence*. In particular, it *offers practitioners a single standard form for evidence gathering, sets strict deadlines, and allows only limited grounds for refusal by the executing State*.

Eurojust supports national authorities throughout the entire life cycle of the EIO – from drafting to execution – by offering guidance and advice. Its National Desks handle large number of cases dealing with EIOs. Feedback collected by Eurojust and the European Judicial Network (EJN) indicates that judicial practitioners generally regard the EIO as a valuable tool.[89]

However, *many Member States were struggling with implementing the EIO Directive in time* and *several issues and challenges related to the practical implementation of the EIO were* identified in cases handled by the National Desks at Eurojust.[90] These issues and challenges, as well as

[89] Eurojust, 'European Investigation Order' (2025) https://www.eurojust.europa.eu/judicial-cooperation/instruments/european-investigation-order accessed 4 August 2025.
[90] See n 6, p. 5.

best practices – particularly those concerning the interception of telecommunications – are addressed in Section 8 of this report.

5.4 Roadmap for lawful and effective access to data for law enforcement

On 24 June 2025, the European Commission presented a Roadmap *setting out the way forward to ensure law enforcement authorities in the EU have effective and lawful access to electronic data*.

In introducing this communication document, the Commission refers to Europol's observation that nearly all forms of serious and organised crime today leave a digital footprint. While around 85% of criminal investigations rely on electronic evidence, requests for data addressed to service providers have tripled between 2017 and 2022 and the need for these data is only increasing. According to the Commission, '*while we have recently seen remarkable examples of law enforcement and judicial authorities successfully cracking down on dedicated criminal communications networks, many more investigations are delayed or unsuccessful due to a lack of timely access to digital evidence. Law enforcement and the judiciary have been losing ground to criminals over the past decade as criminals use tools and products from service providers that have put in place measures preventing cooperation with lawful requests*.'[91]

The Roadmap focuses on six key areas: (a) **data retention** (ensuring the availability of digital evidence), (b) **lawful interception** (obtaining evidence across systems and jurisdictions), (c) d**igital forensics** (retrieving evidence from devices seized in investigations), (d) **decryption** (ensuring that evidence can be read), (e) **standardisation** (reconciling technology and lawful access), and (f) **AI solutions for law enforcement** (analysing evidence effectively and lawfully by using AI).

Lawful access to communication data in real time is referred to in Section II of the Roadmap. The European Commission emphasises - without raising concerns about indiscriminate mass surveillance of telecommunications and its potential impact on the right to privacy - that while demonstrating the critical importance of real-time access to communication content for the effective investigation and prosecution of organised crime groups, the EncroChat case remains one of the few notable success stories. Citing the High-Level Group that prepared the Roadmap, the Commission notes that the effectiveness of lawful interception has significantly declined as communications have shifted from traditional phone calls and SMS to over-the-top (OTT) messaging applications, which now account for approximately 97% of all mobile messages. Following the disruption of major criminal communication networks in 2020, many criminal groups reverted to using standard end-to-end encrypted OTT messaging services.[92]

The Commission highlights that the effective cross-border collection of evidence through telecommunications interception is significantly hindered by fragmented national rules. While some Member States impose similar obligations on all types of electronic communication services, including OTT providers, others exclude them. Moreover, service providers are often not established in the Member State of the requesting authority, creating complex jurisdictional

[91] See n 77.
[92] *Ibid*.

issues, conflicts of law, and enforcement challenges. Consequently, the content of such messaging services is often practically inaccessible.[93]

The Commission also notes that national authorities continue to face difficulties when using the EIO and other cooperation instruments, as these mechanisms cannot support interception when the service is provided from either non-participating Member States or third countries.[94]

Finally, according to Commission, some Member States lack the necessary network infrastructure to support effective cross-border data sharing.[95]

The Commission plans to strengthen cross-border cooperation on lawful interception, focusing on enhancing the EIO. Its main goal is to *ensure that all communication providers offering services in Member States - whether traditional telecoms or internet-based - can be subject to lawful interception obligations, regardless of their location*. By 2027/2028, the Commission intends to:

(a) improve the efficiency of cross-border interception requests through a stronger EIO mechanism;

(b) establish a level playing field for enforcing interception obligations across all communication providers;

(c) *d*evelop strategies to address non-cooperative providers; and

(d) support the rollout of secure information-sharing infrastructure between Member States, Europol, and other security agencies.[96]

In Section IV of the Roadmap, the Commission underscores the *crucial role of encryption and other cybersecurity measures in protecting information systems*. Today, 60–80% of messaging applications are end-to-end encrypted, including widely used services such as WhatsApp, Messenger, Signal, and iMessage, while the global use of SMS and traditional phone calls continues to decline. While encryption enhances the privacy of communications, it simultaneously restricts law enforcement and judicial authorities' ability to collect evidence, rendering most lawful interceptions ineffective.[97]

According to the Commission, Member States currently possess limited and uneven decryption capabilities, with success rates varying from as low as 15–20% to over 66%. Decryption equipment is highly specialised, expensive, and often based on non-EU commercial solutions, which quickly become obsolete and may not meet EU digital forensic standards. High licensing costs restrict the number of authorised users, and the tools are only effective in a small fraction of investigations. Authorities sometimes resort to exploiting device vulnerabilities to obtain decryption keys, which can conflict with the policy goal of ensuring cybersecurity by default. The challenge is further compounded by modern devices using strong encryption, crypto chips, and

[93] *Ibid.*
[94] *Ibid.*
[95] *Ibid.*
[96] *Ibid.*
[97] *Ibid.*

complex passwords, which remain inaccessible even with the most advanced decryption platforms.[98]

To address these challenges, the Commission will *establish an expert group to develop a technology roadmap on encryption*. This roadmap will identify and assess solutions that allow lawful access to encrypted data while safeguarding cybersecurity and fundamental rights. Building on the proven success of Europol's decryption platform in major cases such as Sky ECC and EncroChat, the Commission will *invest in advanced decryption capabilities to ensure that Europol can effectively support Member States well beyond 2030*.[99]

[98] *Ibid*.
[99] *Ibid*.

6. NATIONAL LEGAL FRAMEWORKS

This section examines the national legal frameworks governing telecommunications interception in criminal proceedings, as well as judicial cross-border cooperation between EU Member States, in the four countries participating in the INCEPT project – Slovenia, Bulgaria, Czech Republic and Poland. Data was collected using a standardised form completed by all project partners.

6.1. Slovenia

6.1.1 Provisions on the interception of telecommunications

In the Republic of Slovenia, the legal framework governing the interception of telecommunications is primarily established by the *1991 Constitution*, along with two key legislative instruments: the *Criminal Procedure Act* (adopted in 1993) and the *Electronic Communications Act* (adopted in 2022). The technical aspects of the lawful interception of telecommunications – such as the required interfaces and functionalities of the equipment that service providers must ensure for the lawful surveillance of traditional and electronic communications – are regulated by the *Rules on Equipment and Interfaces for the Lawful Interception of Communications*. Additionally, provisions related to telecommunications interception are also contained in the Slovenian Intelligence and Security Agency Act. However, data obtained by the Slovenian Intelligence and Security Agency (SOVA) through such interception may not be used as evidence in criminal proceedings.[100] The same applies to the Intelligence and Security Service of the Ministry of Defence (OVS MORS).

At a fundamental level, the legal framework for police surveillance of telecommunications in criminal investigations is grounded in constitutional provisions protecting the right to privacy, which explicitly encompasses communication and information privacy. According to the **Constitution**,[101] every individual is guaranteed privacy, including the confidentiality of correspondence and other forms of communication. This protection may only be suspended by statutory law, and solely on the basis of a court order, for a limited period, when necessary for the initiation or conduct of criminal proceedings or for reasons of national security. The protection of personal data is also constitutionally guaranteed. Every individual has the right to access personal data collected about them and the right to judicial protection in cases of misuse.[102]

The interpretation and scope of these constitutional provisions – defining the limits of lawful interference with an individual's communication and information privacy – are shaped by the case law of the Constitutional Court, with the jurisprudence of the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU) also playing a significant role.

[100] In its **Decision Up-412/03-21 of 8 December 2005**, the Constitutional Court of the Republic of Slovenia held that the Slovenian Intelligence and Security Agency (SOVA) lacked the legal authority to carry out the covert measure of wiretapping and recording the telephone conversations of the constitutional complainant, as such measures were reserved exclusively for the police. In the related criminal case, where data obtained through SOVA's wiretapping were used as evidence, the Court found violations of Articles 35 and 37 of the Constitution, which protect the right to privacy and personality rights, as well as the privacy of correspondence and other means of communication. The Court has reaffirmed this position in several subsequent decisions.

[101] The Constitution of the Republic of Slovenia (*Ustava Republike Slovenije*), Official Gazette of the Republic of Slovenia nos. 33/91, 42/97, 66/00, 24/03, 69/04, 68/06, 47/13, 47/13, 75/16, 92/21.

[102] *Ibid*., Arts. 35, 37 and 38.

Explicit provisions on the real-time interception of telecommunications in criminal investigations are set out in the **Criminal Procedure Act (CPA),**[103] specifically in *Chapter XV – Preliminary proceedings* in Articles 149a to 156a on covert investigative measures (CIM). The numerous and often extensive and detailed provisions concern *real-time and retroactive collection* of *content*, *traffic* and *location* telecommunication data.

A central role is played by **Article 150 CPA**, which governs the ***surveillance of telecommunications through wiretapping and recording,*** and the ***surveillance and preservation of evidence on all forms of communication transmitted via electronic communications networks***. This article provides that the surveillance of communications – through wiretapping, recording, and the preservation of evidence from analogue telephone calls and interception of all forms of communication transmitted via electronic communications networks (e.g., communication via mobile phone calls, SMS, MMS, radio, emails and messaging apps such as Skype, WhatsApp, Viber, Telegram etc.) – may be ordered against a person if the following conditions are met:[104]

- ✓ there are reasonable grounds to suspect that the person has committed, is committing, or is preparing or organising the commission of specific catalogued criminal offences;
- ✓ there is reasonable suspicion that a particular means of communication or computer system is being used in connection with the criminal offence; and
- ✓ it can be reasonably concluded that the evidence cannot be obtained by other investigative measures, or that using such alternative measures would endanger human life or health.

The collection of evidence by telecommunications interception may be ordered in connection with:[105]
(a) criminal offences against the security of the Republic of Slovenia and its constitutional order;
(b) criminal offences against humanity and international law for which the prescribed penalty is imprisonment of five years or more;
(c) specifically catalogued criminal offences; and
(d) criminal offences for which a prison sentence of at least eight years is prescribed.

The measure may be ordered by the *investigating judge* in the form of a written order, based on a written proposal submitted by the state prosecutor. Exceptionally, if it is not possible to obtain a written order in time and there is a risk of delay, the investigating judge may issue the order orally, based on a reasoned oral proposal by the public prosecutor. In such cases, a written order must be issued no later than twelve hours after the oral order is given.[106]

The duration of the measure is limited to a maximum of one month. However, for justified reasons, it may be extended by successive one-month periods, up to a total maximum duration of six months.[107]

The court order is executed by the police, and service providers are obliged to enable the police to execute the order. However, the police must cease the implementation of the measure as soon as the reasons for which it was ordered cease. They shall notify the investigating judge in writing

[103] The Criminal procedure Act (*Zakon o kazenskem postopku* [CPA]), Official Gazette of the Republic of Slovenia, nos. 176/21 – officially consolidated text and 53/24.
[104] *Ibid.*, Art. 150, para. 1.
[105] *Ibid.*, para. 2.
[106] *Ibid.*, Art. 152.
[107] *Ibid.*

of the termination without delay. The investigating judge may at any time ex officio, if he or she assesses that there are no longer any reasons for implementing the measure, or that it is being implemented contrary to his or her order, order the implementation of the measure to be stopped by means of a written order.[108]

The provisions of the CPA on CIM related to the real-time interception of telecommunications also include paragraphs one and three of **Article 149c CPA**. These provisions regulate the ***real-time preservation and transmission of communications traffic data by service providers***, as well as the **preservation and transmission of data concerning the location of a communication device or its user**.

Finally, the provisions of the CPA on CIM related to the real-time interception can be found in **Article 150a** on the ***use of IMSI catchers***.

The CPA also contains provisions that, while not directly regulating the real-time interception of telecommunications, are related to it. These provisions concern the preservation, acquisition, and transmission of stored *subscriber data* and communication *traffic data* by service providers or by the owners or users of electronic devices. They include:

- Request for the transmission of stored communication traffic data (Article 149b);
- Request for the transmission of subscriber data (Article 149č);
- Request for the immediate preservation of electronic data (without a court order) in cases where judicial authorisation is otherwise required (Article 149e).

Since the adoption of the CPA in 1993, the provisions on CIM including telecommunication interception have been amended several times. In most cases, these amendments were initiated by the police, who emphasised the need for more effective tools and technical means to prevent, detect, investigate, and prosecute criminal offences and their perpetrators. Some of these amendments were subsequently challenged before the Constitutional Court, which, on several occasions, found them to be inconsistent with the Constitution.

6.1.1.1 Constitutional review of the Criminal Procedure Act provisions related to telecommunications interception

The most recent constitutional review of the CPA provisions concerning telecommunications interception took place in 2022 and 2023. Acting on requests submitted by a group of deputies of the National Assembly, the Constitutional Court issued three partial decisions addressing various provisions on covert investigative measures (CIM), including several related specifically to telecommunications interception.

In its **Second partial decision U-I-144/19 of 1 December 2022**,[109] the Court reviewed the constitutionality of Article 150a CPA. Citing the principles of proportionality and legality in criminal law, the Court annulled most of the article's provisions concerning the use of IMSI catchers, with the exception of those allowing the monitoring of mobile telephony signals solely for the purpose of determining the location of a communication device (see also Section 7.3.1 of this report).

The partially annulled **Article 150a CPA** stipulates that the **police may use special technical means for monitoring mobile telephony signals (e.g., an IMSI catcher) solely for the purpose of determining the location of a communication device**, provided that there are

[108] *Ibid*.
[109] U-I-144/19 (Part Two), adopted on 1 December 2022, Official Gazette of the Republic of Slovenia, No. 2/23.

reasonable grounds to suspect that a specific person has committed, is committing, or is preparing to commit:[110]

- criminal offences against the security of the Republic of Slovenia and its constitutional order;
- criminal offences against humanity and international law are punishable by a prison sentence of five years or more;
- the criminal offence of unlawful deprivation of liberty under Article 133 of the Criminal Code; or
- certain other serious criminal offences specified by law.

Additionally, there must be reasonable suspicion that a particular means of communication is being used in connection with the criminal offence, and it must be reasonably concluded that the location of the perpetrator cannot be determined by other measures, or that doing so would involve disproportionate difficulty.[111]

The use of an IMSI catcher may be ordered by the investigating judge through a written order issued upon a written proposal from the public prosecutor.[112] Exceptionally, if a written order cannot be obtained in time and there is a risk of delay, the investigating judge may issue an oral order upon a reasoned oral proposal from the public prosecutor.[113] A written order must then be issued no later than 12 hours after the oral order is given.[114]

The measure may last for a maximum of one month.[115] The police must terminate the implementation of the measure as soon as the reasons for its application cease to exist. The investigating judge may, at any time and ex officio, order the termination of the measure by written order if they determine that the grounds for its implementation no longer exist or that it is being carried out in violation of the issued order.[116]

The police must implement the use of IMSI catchers in a manner that interferes as little as possible with the rights of individuals who are not suspects.[117]

The **Third partial decision U-I-144/19 of 6 July 2023**[118] of the Constitutional Court concerned, *inter alia*, the constitutionality of the CPA provisions set out in Articles 149b, 149c, and 149č. These articles address the acquisition of subscriber and communication traffic data, including information on interlocutors, the date, time, duration, and destination of communications, telephone numbers, IP addresses or similar identifiers of communication devices provided by the service provider, and the type of service used.[119]

[110] See n 103, Art. 150a, para. 3.
[111] *Ibid*.
[112] *Ibid*, Art. 152, para. 1.
[113] *Ibid*., Art. 152, para. 2.
[114] *Ibid*., para. 4.
[115] *Ibid*., para. 4.
[116] *Ibid*., para. 6.
[117] *Ibid*., para. 7.
[118] Constitutional Court of Slovenia, decision U-I-144/19 (Part Three) Official Gazette 89/23.
[119] The Constitutional Court maintained that these data do not provide insight into the content of the communications, but they can be used to draw a number of conclusions about numerous aspects of the private lives of the persons concerned, such as their daily habits, place of residence, daily or other journeys, activities, social relationships, and the environments they visit. See Constitutional Court of the Republic of Slovenia, Summary of Decision U-I-144/19 (Part Three).

Specifically, the first paragraph of Article 149b permits the retroactive acquisition of communication traffic data relating to a suspect, an injured party, or other persons defined by law. The first paragraph of Article 149c governs the securing and real-time acquisition of traffic data from service providers concerning the communications of these individuals – i.e., data collected during the execution of the measures and going forward. The third paragraph of Article 149c addresses the preservation and transmission of data relating to the location of a communication device or user. Article 149č sets out the service provider's obligation to supply subscriber data regarding the owner or user of a specific means of communication or online or other information society services, as well as information on the existence and content of the contractual relationship with that individual.

The Constitutional Court found that all three provisions constituted interferences with human rights. While the first paragraph of Article 149b and the first paragraph of Article 149c of the CPA interfered with the right to communication privacy, as protected under the first paragraph of Article 37 of the Constitution, the third paragraph of Article 149c interfered with the privacy of a person's location, which falls under the right to information privacy as guaranteed by the first paragraph of Article 38 of the Constitution.[120]

Although the Constitutional Court found that the challenged measures pursued a constitutionally permissible objective – namely, the effective conduct of criminal proceedings – it held, without assessing whether the measures were necessary and appropriate to achieve that objective, that they were excessive and failed to meet the requirement of proportionality in the strict sense.
In this context, the Court emphasised three key concerns:
(a) the evidentiary threshold of 'grounds for suspicion' was unacceptably low;
(b) there was no time limit imposed on the application of the measures; and
(c) the scope of criminal offences for which the measures could be applied was overly broad.

The Court concluded that the severity of the impact these measures would have on the affected human rights outweighed the benefits of pursuing the otherwise constitutionally legitimate aim. Consequently, the Constitutional Court annulled Articles 149b and 149c in their entirety.[121]

The annulment took effect on 12 August 2024, providing the legislature with time to amend the provisions on CIM in accordance with constitutional standards.

6.1.1.2 The 2024 amendments to the Slovenian Criminal Procedure Act (CPA-P)

In January 2024, the Ministry of Justice of the Republic of Slovenia prepared **draft amendments to the Slovenian Criminal Procedure Act (CPA-P)**[122] and circulated them to a broad range of stakeholders for professional consultation. Among other things, the draft aimed to align the provisions on CIM with the Constitutional Court's decision of July 2023.

The Ministry emphasised that, pursuant to the second paragraph of Article 37 of the Constitution and in line with the Constitutional Court's decision, the CPA must establish a clear and general time limit for criminal law interference with communication privacy through the acquisition or access to communication traffic data. This should be done in accordance with the principle of proportionality and with a nuanced approach to interferences with human rights and fundamental freedoms. The Ministry also noted that the Electronic Communications Act already regulates time

[120] *Ibid.*
[121] *Ibid.*
[122] Ministry of Justice (Slovenia), 'Draft amendments to the Criminal Procedure Act' (EVA 2024-2030-0001) https://e-uprava.gov.si/.download/edemokracija/datotekaVsebina/657266?disposition=inline&lang=si accessed 2 August 2025.

limits for the commercial storage of traffic data accessed by the challenged measures. According to the Constitutional Court, setting such limits would also help prevent the potential acquisition of data that, under the Electronic Communications Act, should no longer be stored but may still exist.[123]

Furthermore, the Ministry stressed that any amendments to the current legal framework must take into account relevant case law from the Court of Justice of the European Union (such as *Commissioner of An Garda Síochána*, *La Quadrature du Net and Others*, *Digital Rights Ireland Ltd*., and *Tele2 Sverige AB*) and the European Court of Human Rights (including *Zakharov v. Russia*, *Szabó and Vissy v. Hungary*, and *Benedik v. Slovenia*), as well as the Constitutional Court of the Republic of Slovenia (Decision No. U-I-65/13-19 of 3 July 2014), all of which address limits on state interference with communication privacy rights.[124]

The **CPA-P amendments**[125] were adopted by the National Assembly in June 2024.

The **amended Article 149b CPA**, which allows for the ***request for the transmission of stored communication traffic data***, stipulates that this measure may be ordered if there are reasonable grounds to suspect that a specific or identifiable person has committed, is committing, or is preparing or organising the commission of a criminal offence punishable by a prison sentence of five years or more, or a catalogued criminal offence. Additionally, it must be reasonably concluded that the act cannot be detected, prevented, or proven, nor the perpetrator identified, by other investigative measures or without disproportionate difficulty.

Upon a reasoned proposal from the public prosecutor, the investigating judge shall request the service provider or a third party lawfully in possession of the data in the course of its business to provide the competent authority with the necessary traffic data relating to the suspect's communications. The data must lawfully exist at the time the order is issued and must meet the following temporal limitations:[126]

(a) not older than six months, if the offence is punishable by a prison sentence of eight years or more;
(b) not older than four months, if the offence is punishable by a prison sentence of five years or more;
(c) not older than three months, if the offence is punishable by a prison sentence of less than five years.

Exceptionally, the investigating judge may also order this measure against a person who is not the suspect, if it is absolutely necessary to identify a means of communication likely to be used by the suspect, and it can be reasonably concluded that such identification cannot be achieved by other means or would involve disproportionate difficulty.[127]

In urgent cases, where a written order cannot be obtained in time and delay would endanger human life or health, the investigating judge may, upon a reasoned oral proposal from the state prosecutor, issue an oral order for the execution of the measure. A written order must then be issued no later than 12 hours after the oral order.[128]

[123] *Ibid*.
[124] *Ibid*.
[125] Act amending the Slovenian Criminal Procedure Act – CPA-P (*Zakon o spremembah in dopolnitvah Zakona o kazenskem postopku – ZKP-P*), Official Gazette of the Republic of Slovenia, no. 53/24.
[126] See n 103, Art. 149b, para. 1.
[127] *Ibid*., para. 2.
[128] *Ibid*., para. 4.

The **amended Article 149c CPA**, which regulates the ***real-time preservation and transmission of communication traffic data*** by service providers, provides that this measure may be ordered by an order of investigating judge upon a reasoned proposal from the state prosecutor if there are reasonable grounds to suspect that a specific or identifiable person has committed, is committing, or is preparing or organising the commission of a criminal offence punishable by five or more years of imprisonment, or a catalogued criminal offence. It must also be reasonably concluded that the offence cannot be detected, prevented, or proven, nor the perpetrator identified, through other investigative measures, or that doing so would involve disproportionate difficulty.[129]

The period for which the measure is ordered may not exceed one month. The investigating judge may, by issuing a new order, extend the implementation of the measure for additional periods of up to one month, for a total duration not exceeding six months.[130]

If a telecommunications surveillance measure involving wiretapping and recording under Article 150 of the CPA is also ordered in relation to a specific means of communication, the judge may order the preservation and transmission of traffic data for that same means of communication for the entire duration of the Article 150 measures.[131]

The investigating judge may, exceptionally and in accordance with the principle of proportionality, order the measure also against a person who is not a suspect, including individuals for whom detention, house arrest, a search warrant, or an arrest warrant has been issued but who have fled or are in hiding. In such cases, the order must specify whether the person will be informed of the measure upon its completion or whether, due to the interests of the proceedings, the person will not be informed.[132]

Although the Constitutional Court did not find any inconsistency with the Constitution when assessing **Article 149č CPA**, the CPA-P amendment also interfered with this article. This article stipulates that **a court**, **a state prosecutor or the police may request a service provider in writing to provide, without the consent of the individual to whom the data relate, *subscriber data* on the owner or user of a specific means of communication or online or other information society services, as well as on the existence and content of his contractual relationship**.[133]

This measure may be ordered if there are grounds to suspect that a criminal offence has been committed, is being committed, or is being prepared or organised, for which the perpetrator is prosecuted ex officio, and it is necessary to obtain subscriber data regarding the owner or user of a means of communication or internet service, or information on the existence and content of their contractual relationship with the service provider, in order to detect, prevent, or prove the offence or to identify the perpetrator.[134]

For justified reasons and at its own expense, the service provider may choose to forward the requested data, along with a copy of the request, in writing to the competent court instead of the

[129] *Ibid*., Art. 149c, para. 1.
[130] *Ibid*.
[131] *Ibid*.
[132] *Ibid*., para. 2.
[133] *Ibid*., Art. 149č, para. 1.
[134] *Ibid*.

police or the public prosecutor. Upon receipt, the court shall verify the legality of the categories of data that have been submitted.[135]

Following the CPA-P amendment, the **third paragraph of Article 149č CPA** now provides that ***when subscriber data enable the identification of a person through a unique identifier (such as an IP address) that is not public or in relation to which there is a legitimate expectation of privacy, the acquisition of such data must be ordered by the investigating judge upon a reasoned proposal from the public prosecutor***. The court order may be issued if it can be reasonably concluded that a criminal offence has been committed, is being committed, or is being prepared or organised, and the offence is subject to ex officio prosecution.

This amendment was prompted by the *Benedik v. Slovenia* judgment,[136] in which the European Court of Human Rights held that there had been a violation of Article 8 of the European Convention on Human Rights (the right to respect for private and family life), due to the Slovenian police's failure to obtain a court order before accessing subscriber information associated with a dynamic IP address. According to the Court, the legal provision relied on by the Slovenian police to access such information without prior judicial authorisation did not meet the Convention requirement of being 'in accordance with the law.'[137]

When ordering the measures referred to in Articles 149b, 149c, and 149č CPA, the investigating judge shall, by order, determine a period during which the service provider is prohibited from disclosing to the user, subscriber, or any third party that it has transmitted or will transmit certain data in accordance with these provisions. This period may not exceed 24 months from the end of the month in which the execution of the order was completed. The investigating judge may extend this period by order for a maximum of 12 months on each occasion, but not more than twice.[138]

Additionally, in the context of telecommunications interception, **Article 149e CPA** – which regulates **requests for the immediate preservation of electronic data (without a court order) in cases where judicial authorisation is otherwise required** – is also significant. Notably, this provision remained unchanged in the CPA-P amendment.

Article 149e CPA stipulates that the state prosecutor or the police may, *without prior court authorisation*, request in a written form the owner or user of an electronic device, as well as the service provider or a third party who lawfully holds the data in the course of their business and it is likely that this data may have already been deleted or changed by the time the court order is delivered, to preserve any type of data stored in electronic form until receipt of the court order, but not longer than 30 days from the date of delivery of the request. The state prosecutor or the police may extend the deadline by a maximum of 30 days with an additional request. If a court order is not served within the retention period, the retention of the data shall be terminated.[139]

This measure may be used if there are *grounds to suspect* that a criminal offence has been committed, is being committed, or is being prepared or organised, and if it is necessary to obtain

[135] *Ibid*., para. 2.
[136] *Benedik v Slovenia* App no 62357/14 (ECtHR, 24 April 2018).
[137] The ECtHR dissagreed with the Slovenian Constitutional Court which concluded that the applicant, who had not hidden in any way the IP address through which he had accessed the Internet, had consciously exposed himself to the public and had thus waived the legitimate expectation of privacy.
[138] See n 103, Arts. 149b, para. 5, 149c, para. 5 and 139č, para. 4.
[139] *Ibid*., Art. 149e, para. 1.

data stored in electronic form in order to detect, prevent, or prove the offence or to identify the perpetrator.[140]

Based on Article 149e, service providers may be requested to preserve traffic data and the content of communications only for the purpose of detecting, preventing, or proving criminal offences punishable by a prison sentence of eight years or more, as well as certain serious catalogued criminal offences.90

Exceptionally, if a written request cannot be issued in a timely manner and there is a risk that the data may be destroyed before it is issued, the public prosecutor or the police may order the preservation of the data by means of an oral request. An official record shall be made documenting the submission of the oral request. A written request must be issued no later than 12 hours after the oral request has been made. If the written request is not issued within this time frame, the data preservation measure shall be lifted.[141]

Table 1: Communications interception in Slovenia (competent authorities, standards of proof, duration)

Measure	Competent authority and standard of proof	Initial duration and extension	Maximum duration
Surveillance of telecommunications through wiretapping and recording (phone calls)	Investigating judge upon a reasoned proposal from the state prosecutor (in a written form, exceptionally orally) Reasonable grounds for suspicion	Up to one month Deadline may be extended for additional periods of up to one month	Max. 6 months
Control and preservation of evidence on all forms of communication transmitted via electronic communications networks (SMS, MMS, emails, messaging apps)	Investigating judge upon a reasoned proposal from the state prosecutor (in a written form, exceptionally orally) Reasonable grounds for suspicion	Up to one month Deadline may be extended for additional periods of up to one month	Max. 6 months
Use of IMSI catchers	Investigating judge upon a reasoned proposal from the state prosecutor (in a written form, exceptionally orally – A written order must then be issued no later than 12 hours after the oral order is given) Reasonable grounds for suspicion	Up to one month No extension of the deadline	Max. 1 month

[140] *Ibid.*
[141] *Ibid.*, para. 4.

Measure	Competent authority and standard of proof	Initial duration and extension	Maximum duration
	**The police may use IMSI catchers solely for the purpose of determining the location of a communication device		
Real-time preservation and transmission of communications traffic and location data	Investigating judge upon a reasoned proposal from the state prosecutor Reasonable grounds for suspicion	Up to one month Deadline may be extended for additional periods of up to one month	Max. 6 months
Request for the transmission of stored communication traffic data	Investigating judge upon a reasoned proposal from the state prosecutor (in a written form, exceptionally orally) Reasonable grounds for suspicion		**The data must meet the following temporal limitations: (a) must not be older than 6 months (if crime is punishable by 8 years prison sentence) of 8 years or more (b) must not ne older than 4 months, (if 5 or more years prison sentence (c) must not be older than 3 months (if prison sentence of less than five years)
Request for the transmission of subscriber data	Court, state prosecutor, the police (in a written form) Grounds for suspicion		
Request for the immediate preservation of electronic data (without a court order) in cases where judicial	State prosecutor, the police (in a written form, exceptionally orally) Grounds for suspicion	Until receipt of the court order, but max. 30 days from the date of delivery of the request	Until receipt of the court order, but max. 60 days from the date of delivery of the request

Measure	Competent authority and standard of proof	Initial duration and extension	Maximum duration
authorisation is otherwise required		Deadline may be extended by a max. of 30 days	

6.1.1.3 The Electronic Communications Act (ZEKom-2)

The **Electronic Communications Act (ZEKom-2)**[142] is the principal piece of legislation regulating electronic communications in Slovenia. The current version, ZEKom-2, was adopted in 2022, replacing the previous ZEKom-1. It aligns Slovenian national legislation with EU law, particularly the European Electronic Communications Code (EECC) (Directive (EU) 2018/1972), which aims to harmonise telecommunications regulation across the European Union.

Article 128 of ZEKom-2 stipulates that service providers must enable the lawful interception of communications at a designated point in the public communications network immediately upon receiving an order from a competent authority. The interception must be carried out in the manner, to the extent, and for the duration specified in the order. Exceptionally, and if provided for under the CPA, service providers must also comply with lawful interception requests based on oral orders.

Service providers are required to maintain an indelible record of every lawful interception for a period of 30 years. At their own expense, they must install appropriate equipment and suitable interfaces within their networks to enable lawful interception. This obligation also extends to international communications: service providers must provide, again at their own expense, the necessary equipment and delivery interfaces to support the lawful interception of cross-border communications.

6.1.1.4 Oversight and control

The use of SIM, including telecommunications interception, is subject to internal, administrative, judicial, and parliamentary oversight, as well as oversight by independent supervisory bodies.

Internal and administrative oversight

The police are considered the most closely supervised authority within the Slovenian legal system. The legal framework also provides for internal oversight of the legality of police powers and measures (including CIM), as well as regular and extraordinary supervision, which is carried out by the Ministry of the Interior through the Police Guidance and Supervision Sector. In addition, a formal complaints procedure against police conduct has been established within both the police force and the Ministry of the Interior.

Judicial oversight

[142] The Electronic Communications Act (*Zakon o elektronskih komunikacijsh* [ZEKom-2]), Official Gazette of the Republic of Slovenia, no. 130/22.

Judicial supervision is carried out by courts of general jurisdiction (e.g., district courts, appellate courts, and the Supreme Court) and the Constitutional Court. Upon termination of telecommunications interception measures under Articles 149b, 149c, 149č, 150, and 150a of the CPA, the police are required to submit the data and recordings, along with a report, to the state prosecutor. The state prosecutor then forwards all materials obtained through these measures to the investigating judge, who operates within the district courts.

The investigating judge must examine whether the measures were implemented in the manner in which they were approved.[143] The state prosecutor is required to hand over the seized material to the investigating judge even if no criminal proceedings are initiated against the suspect.[144] Recordings and data obtained through telecommunications interception, along with related documentation, must be retained by the court for the purpose of ensuring the effective conduct of criminal proceedings and safeguarding the suspect's or defendant's right to defence. These materials must be preserved for as long as the criminal file is maintained or until it is destroyed.[145]

If the state prosecutor initiates criminal proceedings against a suspect who has been subject to investigative measures, or if the suspect is arrested, the investigating judge must inform the suspect of the measures taken and the information collected no later than the filing of the indictment or immediately after the arrest.[146]

If the state prosecutor declares that criminal prosecution will not be initiated against the suspect, or if no action, measure, or investigative act aimed at prosecuting the suspect is proposed, ordered, or carried out within **two years**, the collected material shall be destroyed under the supervision of the investigating judge.[147] Before the destruction, the investigating judge shall inform the suspect and any other persons against whom the measures were implemented of their use. If the injured party assumes the role of a subsidiary prosecutor, the collected material shall not be destroyed.[148]

If telecommunications interception measures were carried out without an order from the investigating judge or in violation of such an order, the court may not base its decision on the recordings or data obtained through those measures.[149]

In the Slovenian criminal procedure system, once the indictment becomes final, a pre-trial hearing is held, during which the defendant may request the exclusion of evidence obtained through telecommunications interception if the evidence is deemed inadmissible.[150] The defendant may also challenge such evidence – whether obtained through real-time telecommunications interception or related measures – during the main hearing and subsequently in an appeal against the judgment. Under certain conditions, the defendant may also object to its admissibility in proceedings involving extraordinary legal remedies.

After all regular and extraordinary legal remedies have been exhausted, any individual who believes that their fundamental rights were violated during the course of criminal proceedings may file a constitutional complaint with the Constitutional Court. If the individual can demonstrate

[143] See n 103, Art. 153, para. 2.
[144] *Ibid*., para. 4.
[145] *Ibid*., 154, para. 4.
[146] *Ibid*., para. 2.
[147] This deadline is preclusive (see Supreme Court judgment VSRS I Ips 15930/2017 of 31 May 2018).
[148] See n 103, Art. 154, para. 2.
[149] *Ibid*., para. 4.
[150] *Ibid*., Art. 285d, para. 2.

a legal interest, they may also initiate a constitutional dispute, in which the Constitutional Court reviews the constitutionality of the legal provisions that served as the basis for the conviction.

As a final recourse, an individual convicted of a criminal offence who believes that the conviction was based on telecommunications interception in violation of their fundamental rights may lodge an application with the European Court of Human Rights.

Parliamentary and independent oversight

Parliamentary oversight of the implementation of covert investigative measures (CIM), including telecommunications interception, is regulated by the Act on Parliamentary Oversight of Intelligence and Security Services (ZPNOVS).[151] Oversight under this Act is exercised by the Commission for the Oversight of Intelligence and Security Services. The Commission is responsible for overseeing the intelligence and security services of both the Government and the Ministry of Defence, as well as the security services of the Ministry of the Interior (and the Ministry of Defence).[152] As part of its mandate, the Commission also oversees the use of CIM carried out by the state prosecution and police in the context of criminal investigations.

In addition to judicial and parliamentary oversight, supervision of state prosecution and police activities such as communication interception in is also conducted by independent bodies such as the Ombudsman and various non-governmental organisations.

6.1.1.5 Summary and conclusion

In Slovenia, the legal framework governing the interception of telecommunications is primarily established by the Constitution, the Criminal Procedure Act (CPA) and the Electronic Communications Act.

Since the adoption of the CPA in 1993, the provisions on covert investigative measures (CIM), including telecommunications interception, have been amended several times. Some of these amendments were subsequently challenged before the Constitutional Court, which, on several occasions, found them to be inconsistent with the Constitution.

All measures implying real-time interception of telecommunications require prior judicial authorisation by an investigating judge, ensuring compliance with human rights standards. Real-time interception of telecommunications can be authorised when investigating serious crimes. The CPA determine different authorities and establishes different standards of proof for ordering various measures related to telecommunications interception. In accordance with the principle of proportionality, a higher standard of proof – such as reasonable grounds for suspicion – is required for more intrusive measures, including those involving the interception of content, traffic, and location data. Conversely, a lower standard – grounds for suspicion – applies to less invasive measures, such as the acquisition of subscriber data.[153]

[151] The Oversight of Intelligence and Security Services Act (*Zakon o parlamentarnem nadzoru obveščevalnih in varnostnih služb* [ZPNOVS]), Official Gazette of the Republic of Slovenia, no. 93/07 – officially consolidated text.
[152] ZPNOVS, Art. 3, para. 2.
[153] Following the Constitutional Court decision of 6 July 2023, the amendment CPA-P introduced a higher standard of proof (e.g., reasonable grounds for suspicion) for the retroactive acquisition of stored communication traffic data (Article 149b) and preservation and acquisition of traffic data concerning the communications in real time (Article 149c).

A lower standard of proof is also sufficient for the preservation of all types of stored electronic data. Similarly, reflecting the principle of proportionality, the CPA provides that the acquisition of subscriber data may be ordered not only by the investigating judge but also by the state prosecutor or the police, without a court order, for all criminal offences prosecuted ex officio. In contrast, the acquisition of content, traffic, and location data is permitted only on the basis of a court order issued by the investigating judge and only in connection with offences punishable by longer prison sentences or classified as catalogued crimes.

All measures related to communications interception are now subject to clearly defined time limits. Duration of real-time interception of telecommunication, as well as real-time preservation and transmission of communications traffic and location data, is limited to up to one month, with the possibility of an extension for additional periods of up to one month until a maximum of six months. The use of IMSI catchers is limited to determining the location of a communication device and may last up to one month.

The use of CIM, including telecommunications interception, is subject to internal, administrative, judicial, and parliamentary oversight, as well as oversight by independent supervisory bodies.

Current criminal procedure law in Slovenia does not provide for or allow the remote access to or hacking of electronic devices through the deployment of spyware to infiltrate a suspect's computer, smartphone, or tablet (e.g., **'Trojan horse' surveillance**).[154] Just recently, representatives of the police, along with some legal and security experts, have repeatedly expressed concerns that the Slovenian CPA, unlike the criminal procedure laws of certain other European countries, does not permit Slovenian investigators to use modern technologies to obtain evidence. The Slovenian CPA, they argue, places excessive emphasis on the protection of fundamental rights, at the expense of the effective detection, investigation, and prosecution of the most serious crime committed by individuals and organised criminal groups.[155]

The police are reportedly particularly limited when it comes to intercepting encrypted telecommunications,[156] where traditional interception methods – relying on the cooperation of telecommunications service providers – prove ineffective. They also warn that inadequate procedural legislation poses obstacles to effective cross-border cooperation in criminal investigations.

6.1.2 Provisions on cross-border judicial cooperation related to interception of telecommunications

6.1.2.1 The Act on Cooperation in Criminal Matters with Member States of the European Union

[154] Potential bypass to the absence of explicit provision allowing for the use of Trojan horse surveillance might be in point 3 of the first paragraph of Article 150 CPA which provides for the control of the computer system of a 'bank or other legal entity,' which also includes the installation of a so-called 'forensic computer program' on a computer system that enables the establishment of control over that device (e.g., computer system).
[155] Apollonio D, 'Criminal police drive with the handbrake on [Kriminalistična policija vozi z ročno zavoro]' (2024) 45 Pravna praksa.
[156] The debate over the (in)adequacy of legislation governing telecommunications interception in Slovenia's mainstream media was further intensified by a recent incident at Maribor Prison, where the alleged leader of a dangerous criminal organization, while in custody, reportedly gave instructions to his fellows outside the prison walls using a mobile phone with an encrypted communication app.

The primary piece of legislation in Slovenian domestic law that facilitates cross-border judicial cooperation in criminal matters between EU Member States – including cross-border access to and exchange of electronic evidence through telecommunications interception – is the **Act on Cooperation in Criminal Matters with Member States of the European Union (ZSKZDČEU-1).**[157] This Act aligns Slovenia's legal framework with various EU instruments on mutual legal assistance and ensures efficient and standardised procedures in cross-border criminal cases. Since its enactment, the Act has been amended three times (in 2015, 2018, and 2021) to incorporate new EU directives and framework decisions, thereby ensuring that Slovenia's legal system remains aligned with the evolving EU standards on judicial cooperation.

The Act provides, among other things, for the mutual recognition and enforcement of decisions issued by judicial authorities concerning the arrest and surrender of persons, the seizure and confiscation of objects, the temporary freezing and confiscation of assets, the enforcement of custodial sentences and alternative sanctions, detention, the European Investigation Order, and other related matters.

6.1.2.2 The European Investigation Order

Chapters 8 and 9 of the Act transpose **Directive 2014/41/EU regarding the European Investigation Order (EIO) in criminal matters**[158] into the Slovenian internal legal system. These chapters set out the rules governing both incoming and outgoing European Investigation Orders – that is, the procedures for requesting or executing one or more investigative measures in accordance with the CPA or the Minor Offences Act**.**

The provisions of the Act closely mirror those of the EIO Directive, ensuring harmonised implementation in line with EU standards. The Act defines key terms and establishes the scope, competent authorities, and procedures for issuing and executing EIOs. It also regulates the content of the EIO, grounds for refusal of recognition and execution, consultation processes, conditions for applying alternative investigative measures, time limits for recognition and execution, the decision-making process, notifications, transmission of evidence, use of personal data, the criminal and civil liability of authorities from other Member States, and the allocation of costs.[159] The Act includes 18 annexes, among them *Annexes A, B, and C of the Directive*. These annexes govern how interception requests are issued, transmitted, and executed, including requirements for judicial authorisation, data protection, and respect for national rules on privilege or confidentiality. Annexes A and B relate to the standard EIO form, while Annex C specifically concerns the interception of telecommunications.

Issuing outgoing EIOs

According to the Act on Cooperation in Criminal Matters with EU Member States, the competent authority for issuing an outgoing EIO is the authority empowered to order the specific investigative measure or action under the CPA or the Minor Offences Act. These authorities include:

- the investigating judge,
- the state prosecutor's office, and

[157] The Act on Cooperation in Criminal Matters with Member States of the European Union (*Zakon o sodelovanju v kazenskih zadevah z državami članicami Evropske unije* [ZSKZDČEU-1]), Official Gazette of the Republic of Slovenia, nos. 48/13, 37/15, 22/18, 94/21. Specific provisions on telecommunication interception are enshrined in Title III, articles 17-22.
[158] See n 3.
[159] See n 107, Arts. 59-77.

- the court (during the main hearing).[160]

The police may submit a proposal for issuing an EIO, but it must be approved by the authority competent to order the corresponding investigative measure or action (e.g., the investigating judge or the state prosecutor), or by a district judge in minor offence proceedings.[161]

A competent authority may issue an EIO if the following two basic conditions are met:

(a) the acquisition of evidence is necessary and proportionate for the conduct of criminal or minor offence proceedings, considering the rights of the suspect or accused; and

(b) the execution of the investigative measure or action would be permissible in a similar domestic case under Slovenian law.[162]

In cases involving the interception of telecommunications, an outgoing EIO may be issued exclusively by an investigating judge.[163]

Executing incoming EIOs

The **investigating judge of the district court with territorial jurisdiction over the location where the measure is to be carried out** or the **state prosecutor's office** is competent to decide on an incoming EIO issued for the purposes of criminal proceedings, while the **county court** is the competent authority for EIOs issued in the context of minor offence proceedings.[164]

If the competent authority confirms the EIO, it shall simultaneously determine the manner of execution and order the appropriate measures for its implementation.[165]

As a general rule, an *incoming EIO shall be recognised and executed in the same manner and under the same conditions as if the investigative measure or action had been ordered by a competent Slovenian authority*, subject to certain exceptions.[166]

As in the case of the outgoing EIO, in cases involving the interception of telecommunications, an incoming EIO may be recognised exclusively by an investigating judge.[167]

The grounds for refusal of recognition and execution of an EIO, as set out in the Act on Cooperation in Criminal Matters with EU Member States, reflect the grounds for non-recognition or non-execution established in Article 11 of the EIO Directive.

6.1.2.3 The European Investigation Order for the surveillance of telecommunications

The Act on Cooperation in Criminal Matters with EU Member States includes special provisions for certain investigative measures, including:

- EIOs for the interception of telecommunications *with the technical assistance of another Member State* (Article 30 EIO Directive),

[160] *Ibid*., Art. 73, para. 1.
[161] *Ibid*., para. 2.
[162] *Ibid*., para. 1.
[163] *Ibid*., Art. 77i, para. 1.
[164] *Ibid*., Art. 64, paras. 1 and 2.
[165] *Ibid*., Art. 66, para. 1.
[166] *Ibid*., Art. 65, para. 2.
[167] *Ibid*., Art. 77j, para. 1.

- EIOs for the interception of telecommunications *with the technical assistance of the Republic of Slovenia* (Article 30 EIO Directive), and
- Notification of a Member State where the subject of the interception is located, but *from which no technical assistance is required* (Article 31 EIO Directive). [168]

Outgoing EIO for the surveillance of telecommunications

The **investigating judge** may issue an EIO for the surveillance of telecommunications in another Member State whose technical assistance is required. When issuing it, it shall state why the envisaged investigative measure is relevant for the specific criminal proceedings. The EIO shall be sent to the Member State in which the person whose telecommunications are to be intercepted is or will be present.[169]

The outgoing EIO must contain the following information:

- information for the purposes of identifying the person whose telecommunications are to be monitored;
- the desired duration of the telecommunications monitoring and
- sufficient technical data (in particular the number or other form of identification of the electronic means of communication) to ensure the execution of the EIO.[170]

When issuing an EIO or during an interception, the domestic court may, where it has a special reason to do so, also request the transcription, decoding or decryption of the recording, if the executing authority agrees to this.[171]

In accordance with Article 21 of the EIO Directive, the *executing State shall bear all costs related to the execution of an EIO on its territory*. If the competent Slovenian authority receives a notification from the executing judicial authority of another Member State indicating that the costs associated with executing the EIO are exceptionally high, it shall enter into consultations with the executing authority and either propose a cost-sharing agreement or amend the EIO accordingly. If no agreement is reached, the competent Slovenian authority may withdraw the EIO, in whole or in part.[172]

Incoming EIO for the surveillance of telecommunications

An EIO for the interception of telecommunications with technical assistance in the Republic of Slovenia shall be recognised and ordered to be executed by the **investigating judge** *under the conditions and for the duration specified in the CPA*.[173] The competent court shall consult with the investigating judge whether the order shall be executed:

(a) by the direct transmission of the telecommunications to the issuing State or

(b) by the surveillance of the telecommunications and subsequent transmission to the issuing State.[174]

The investigating judge shall take into account the *general grounds for non-recognition or non-execution* as set out in Article 62 of the Act. **In addition, the execution of an EIO for the**

[168] *Ibid*., Arts. 77i, 77j and 77k.
[169] *Ibid*., Art. 77i, paras. 1 and 2.
[170] *Ibid*., para. 3.
[171] *Ibid*., para. 4.
[172] *Ibid*., Art. 70b.
[173] *Ibid*., Art. 77j, para. 1.
[174] *Ibid*., para. 2.

interception of telecommunications shall be refused if the investigative measure would not have been authorised in a comparable domestic case. The domestic court may also make its consent conditional upon the fulfilment of any requirements that would apply in a similar domestic context.[175]

The *costs incurred in connection with the execution of an EIO shall be borne by Slovenia*, as the executing State, except for the costs of transcription, decoding, and decryption of intercepted communications, which shall be borne by the issuing State.[176]

Notification when no technical assistance is needed (Article 31 EIO Directive)

When the number or other form of identification of the electronic means of communication of a person subject to telecommunications monitoring – pursuant to an order issued by an investigating judge – is used within the territory of another Member State, and *no technical assistance from that Member State is required*, the authority conducting the monitoring shall immediately inform the public prosecutor. The *public prosecutor shall then formally notify the competent authority of that Member State.*[177] The law further specifies when such notification is required – whether prior to the monitoring, at the time of its authorisation, during its execution, or after it has concluded.

Where the person whose telecommunications are being monitored is located in the territory of the Republic of Slovenia, but the *Republic of Slovenia is not providing technical assistance in carrying out the investigative measure*, the District Court in Ljubljana shall be the competent authority to receive the notification from the judicial authority of another Member State. After consulting the competent public prosecutor, the court shall, within 96 hours of receiving the notification, inform the competent authority of the Member State conducting the monitoring:

- whether it does not authorise the monitoring or requires its termination because it would not have been authorised in a similar domestic case; and
- whether the data already obtained through the monitoring while the person was on the territory of the Republic of Slovenia may not be used, or may be used only under conditions determined by the competent Slovenian court.[178]

6.1.2.4 EIO statistics

The data were obtained from the Ministry of Justice, to which – pursuant to Article 8 of the Act on Cooperation in Criminal Matters with EU Member States – the *Supreme State Prosecutor's Office* and the *Supreme Court of the Republic of Slovenia* are required to provide information on cooperation procedures conducted (i.e. by all prosecutor's offices and courts) under the Act. However, the Act does not clearly specify which types of information these institutions must submit to the Ministry with respect to EIOs.

Regarding EIOs within the competence of the prosecution, we received data on the number of issued/rejected outgoing EIOs, as well as the number of received and confirmed/rejected incoming EIOs.

[175] *Ibid.*, para. 3.
[176] Ibid., para. 4.
[177] *Ibid.*, Art. 77k, para. 1.
[178] *Ibid.*, para. 3.

For the judiciary, in relation to incoming EIOs, we received data on the overall number of requests received and the number of confirmed/rejected requests. However, in relation to outgoing EIOs, we were only provided with the number of EIOs issued.

The Ministry assured us that the statistics provided represent the full extent of EIO-related data currently in their possession.

Table 2: Number of EIOs issued and received by the State Prosecutor's Office (Slovenia)
Source: Ministry of Justice of the Republic of Slovenia

YEAR	ISSUED	REJECTED	RECEIVED	REJECTED
2021	206	3	96	1
2022	184	3	82	6
2023	210	3	78	1
2024	248	8	89	3
TOTAL	**848**	**17**	**345**	**11**

Table 3: Number of EIOs issued and received by courts (Slovenia)
Source: Ministry of Justice of the Republic of Slovenia

YEAR	ISSUED	REJECTED	RECEIVED	REJECTED
2021	720	n/a	460	38
2022	766	n/a	341	26
2023	597	n/a	320	33
2024	714	n/a	549	69
TOTAL	**2797**		**1670**	**166**

The tables indicate that courts have issued and received significantly more EIOs than prosecutors' offices. This reflects the fact that, under the CPA, most investigative actions and covert investigative measures during criminal investigations and proceedings are ordered by the judiciary.

Over the past four years, the number of outgoing EIOs issued by investigative and trial judges has ranged between 700 and 800 per year, with the exception of 2023, when a slight decrease was recorded. The number of incoming EIOs reached its highest point in 2024, totalling 549. In previous years, the number of incoming EIOs averaged nearly half the volume of outgoing EIOs. The proportion of rejected incoming EIOs has varied between 7.6% and 17.5% since 2021.

The number of outgoing EIOs issued by prosecutors has been steadily increasing since 2022. In contrast, the number of requests from competent authorities of other Member States for the execution of investigative actions and measures in the Republic of Slovenia has been declining since 2021, although it rose again last year, nearly returning to the level recorded five years ago.

The share of rejected incoming and outgoing EIOs issued by prosecutors has remained negligibly low in all years, ranging between 1% and 7.3% for incoming EIOs and between 1.4% and 3.2% for outgoing EIOs. Interestingly, these figures are significantly lower than those observed in the judiciary. As previously noted, however, the available judicial data only covers incoming EIOs (i.e. requests from other Member States for the execution of investigative measures in Slovenia), with no rejection data available for outgoing EIOs.

In June 2025, three researchers from ZRS Koper conducted an informal interview with the Head of the Investigative Department and a senior investigative judge from the District Court of Ljubljana. We learned firsthand that EIOs issued by investigating judges from the Ljubljana District Court are very rarely rejected by the competent authorities of other Member States. Moreover, the investigative judges explained that outgoing EIOs typically refer to multiple related investigative measures, rather than just a single action. They noted that Slovenian courts do not maintain records of EIOs by specific types of investigative measures, and therefore, they are unable to provide data on the number or proportion of EIOs involving telecommunications interception.

6.2. Bulgaria

6.2.1 Provisions on the interception of telecommunications

6.2.1.1 Overview of the legal framework

In Bulgaria, real-time telecommunications interception is primarily regulated by the Constitution of the Republic of Bulgaria (Article 32 on privacy protections), the Criminal Procedure Code (CPC)[179] and the Special Intelligence Means Act (SIMA)[180]. Provisions that are relevant for interception of telecommunications can also be found in the Electronic Communications Act (ECA). These laws establish the legal framework for the use, authorisation, and oversight of real-time telecommunications interception and other special intelligence means in the context of criminal investigations.

The **Special Intelligence Means Act** is the primary law governing the use of special intelligence means (SIM) in Bulgaria. The law distinguishes between technical means and operational means as part of the SIM for the production of material evidence. Technical means are electronic and mechanical devices, and substances used for documenting the actions of controlled individuals and objects. Operational means are surveillance, wiretapping, tracking, infiltration, the marking and inspection of correspondence and computerised information, controlled delivery, covert investigation and the simulated deal. The law defines the conditions under which SIM can be used, ensuring proportionality and necessity in line with constitutional and European human rights standards. The competent authorities allowed to request and conduct SIM operations include the district prosecutor's offices as well as competent bodies of the Police, the Ministry of the Interior, the State Agency for National Security, the Military Intelligence and the Military Police, the State Intelligence Agency, and the Commission for Combating Corruption. Requests may also be made by the European Prosecutor or Delegated European Prosecutor. A court must authorise the application of SIM before it is implemented, except in urgent cases where ex post judicial approval is required.

The **Criminal Procedure Code** of Bulgaria provides the general procedural framework for criminal investigations, including the use of special intelligence means (SIM) for covert surveillance and interception of communications. Article 172 et seq. regulates the use of SIM as part of pre-trial proceedings. SIM, including real-time interception of telecommunications, can be authorised when investigating serious crimes (e.g., terrorism, organised crime, drug trafficking, corruption). Such measures require prior judicial authorisation by a court, ensuring compliance with human rights standards.

6.2.1.2 Special intelligence means and telecommunications interception

In contrast to Slovenia, where intelligence means and investigative measures in criminal investigation are strictly separated, under Bulgarian national law, telecommunications interception in criminal investigations falls within the category of Special Intelligence Means (SIM), primarily defined in SIMA, not in CPC. Article 2 of this law distinguishes between technical means and operational means as part of the SIM for the production of material evidence. Technical means are defined as electronic and mechanical devices and substances, used for documenting the actions of controlled individuals and objects. Among operational means, SIMA defines the following ones: surveillance, wiretapping/eavesdropping, tracking, infiltration, the marking and

[179] Criminal Procedure Code (Bulgaria), State Gazette of Bulgaria 86/2005.
[180] Special Intelligence Means Act (Bulgaria), State Gazette of Bulgaria 79/1997.

inspection of correspondence and computerised information, controlled delivery, covert investigation, and the simulated deal. [181]

The **core provision related to real-time telecommunications interception** can be found in Article 6 SIMA on 'wiretapping/eavesdropping.' This operational mean is defined as '*the use of technical, auditory or other means for the perception of oral, telephonic or electronic communication of controlled persons*.' Other relevant provisions for real-time telecommunications interception can also be found in Articles 2-5 and 7-10 SIMA, Article 172 et seq. CPC and in the ECA.

The measures referred to in these provisions include **(a) real-time interception of the content of telephone and internet communications** and **(b) metadata collection regarding telecommunications** (traffic and location data such as call records, location of the communication device, IP addresses, and duration of communication). By these measures, authorities can intercept, record, and monitor live telephone calls and online communications such as emails, VoIP calls (e.g., Skype, WhatsApp, Viber), and instant messaging apps and collect traffic and location data (e.g., call records, location data, IP addresses, and duration of communication).

While the use of **IMSI catchers** to intercept mobile phone communications and track their location in real-time is not explicitly regulated under Bulgarian law, law enforcement may use such technology under general SIM provisions, requiring judicial authorisation. Similarly, deployment of spyware which enables remote access and hacking of electronic devices (**'Trojan horse' surveillance** to infiltrate a suspect's computer, smartphone, or tablet) is also not explicitly regulated in Bulgarian law. However, according to the information provided by the project partner, it may be indirectly covered under general provisions on SIM use.

Pursuant to Article 172 et seq. of the CPC, telecommunications interception as well as other types of SIM can be applied in criminal investigations when needed for the investigation of catalogued serious crimes (e.g., terrorism, organised crime, drug trafficking, corruption) committed with intent.[182]

Telecommunications interception and other measures can be applied when the relevant circumstances cannot be established in any other way, or it would involve extreme difficulties. These measures must only be used when less intrusive methods are insufficient for achieving investigative objectives (principle of proportionality and necessity). A *justified request shall be made by the prosecutor to the court* to apply them in pre-trial proceedings. Before submitting the request, the prosecutor is obliged to notify the administrative head of the respective prosecutor's office.[183] In urgent cases, law enforcement may initiate communications interception as well as other SIM without prior authorisation, but a court must approve the action retrospectively within 24 hours. Telecommunication service providers must assist in the interception process.

[181] *Ibid*., Arts. 2-10.
[182] The catalogued crimes include criminal offences under Chapter 1, Chapter 2, Sections I, II, IV, V, VIII and IX, Chapter 3, Section III, Chapter 5, Sections I-VII, Chapter VI, Sections II-IV, Chapter 8, 8a, 9a, Chapter 11, Sections I-IV, Chapter 12, 13, 14 of the Criminal Code, as well as for the crimes under Art. 219 (4), second option, Art. 220 (2), Art. 253, Art. 308 (2), (3) and (5), second sentence, Art. 321, Art. 321a, Art. 356k and Art. 393.
[183] In cases within European Public Prosecutor (EPPO)'s competence, the request is made by the European prosecutor or the European delegated prosecutor.

In criminal investigations involving national security issues, SIMA allows the State Agency for National Security (SANS) to intercept telecommunications and apply other SIMs with its own internal authorisation and extension without strict judicial oversight.

All types of SIM, including communications interception, may also be applied with respect to a witness in the criminal proceedings if they have consented to participate in the establishment of the criminal activity of other persons under Article 108a (terrorism), 143-143a (coercion), 159a-159d (trafficking in human beings), 301-305 (bribery) and 321 (organised criminal group) of the Criminal Code.

Initial authorisation for interception of telecommunications (and other SIM) is granted for up to 2 months in cases: (a) with respect to persons for whom evidence has been received and there are *grounds to suspect* that they are preparing, committing or have committed a serious intentional offence; (b) with respect to persons for whom evidence has been received and there are *grounds to suspect* that they are being used by the latter without knowledge of the criminal nature of the activity carried out; (c) with respect to persons and objects on *grounds of national security*. If needed, an extension may be requested for another 4 months, but only under strict judicial review. The maximum total duration cannot exceed 6 months, except for national security investigations (i.e. terrorism-related cases).[184]

Table 4: Duration of communications interception

Measure	**Initial Duration**	**Extension**	**Maximum Duration**
Telecommunication interception (phone calls, emails, messaging apps)	**Up to 2 months**	Up to **4 additional months** (in two-month increments)	**6 months total** (except terrorism cases)
Metadata collection (traffic and location data)	**Up to 2 months**	Up to **4 additional months**	**6 months total**
National security investigations	**Up to 6 months**	Can be extended indefinitely (internal approval by SANS)	**No strict time limit**

The application of all types of SIM including communications interception shall be discontinued when: (a) the aim has been achieved, (b) the application does not yield results, (c) the term allowed has ended, (d) there is a risk for uncovering the operative means, (e) their application is impossible, (f) there is a risk for the life and health of the undercover agent or for his immediate family due to the relating tasks.[185]

When the use is discontinued, the authority who has allowed them shall be immediately notified. If the information collected up to this point will not be used for producing material evidence, they order its destruction.

[184] When applied with respect to objects for the purpose of establishing the identity of individuals for whom information was received of being involved in alleged criminal activities, the term to apply SIM is up to 20 days. This term can be extended with 20 more days but for no more than 60 days in total.
[185] See n 179, Art. 175.

When evidence is being produced, this is done in 2 copies which have to be sent within 24 hours of being prepared to the requesting prosecutor and to the allowing court in sealed packages. If needed, the prosecutor may request more copies.[186]

According to the Bulgarian criminal procedural law, the indictment and the conviction cannot be based on SIM alone. Furthermore, the information received through the usage of telecommunication interception or/and other SIM shall be limited with respect to the purposes of the initial request made (e.g. for what it was issued) unless it contains evidence for another serious crime committed with intent if for these crimes such measures are allowable. Information received when applying SIM in one set of criminal proceedings may be used in another set of criminal proceedings as evidence for such serious and intentional crime being committed.[187]

6.2.1.3 Legal admissibility and oversight

Legal admissibility of telecommunications interception and other CIM results as evidence in court is subject to strict legal conditions. The results can only be used if the measure was conducted under valid judicial authorisation, the evidence was lawfully obtained and the evidence is relevant to the criminal case. The original audio recordings, transcripts, videos, and metadata must remain unaltered. The prosecution must present the evidence within the statutory deadlines to avoid exclusion. If telecommunication interception or other CIM was conducted without proper authorisation, its results cannot be used in court (exclusionary rule). However, in some cases, unlawfully obtained evidence may still be used if it is crucial for proving a serious crime.

If SIM, including telecommunications interception, result in irrelevant or non-incriminating evidence, the data must be deleted within 10 days. Collected evidence can only be used in court if it is lawfully obtained. Unauthorised use or disclosure of intercepted data is punishable.

CIM, including telecommunication interception results, must be presented during the pre-trial phase and included in the case file before indictment. If the evidence is not used within 5 years, it must be deleted or classified, unless related to ongoing national security threats. In cases of acquittal or dropped charges, telecommunication interception and other CIM records must be permanently destroyed.

6.2.1.4 Constitutional review of the Electronic Communications Act and the Special Intelligence Means Act provisions related to telecommunications interception

Bulgaria's normative framework for CIM and telecommunications interception has undergone constitutional review. More particularly, the Constitutional Court has addressed issues related to data retention and surveillance practices.

In landmark **Decision No. 1/2005**, the Constitutional Court dealt with the constitutionality of the SIMA. The Constitutional Court examined the legal provisions related to the interception of telecommunications and their compliance with constitutional rights, particularly the right to privacy. The Court affirmed the legality of intercepting communications under strict conditions, including judicial oversight and proportionality of the measures. It stressed the need for balancing public safety with the protection of individuals' privacy.

In the **Decision of March 12, 2015**, the Constitutional Court declared certain provisions of the ECA unconstitutional. These provisions mandated the bulk collection of telecommunications data, requiring service providers to retain all traffic data for one year, extendable by six months upon

[186] *Ibid*., Art. 176.
[187] *Ibid*., Art. 177.

law enforcement request. The Court found that such indiscriminate data retention violated the constitutional protection of privacy and personal data. The Court's decision necessitated legislative amendments to align data retention practices with constitutional standards. This led to a more targeted approach, limiting data retention to specific cases with judicial oversight, thereby enhancing the protection of individual privacy rights.

6.2.2 Provisions on cross-border judicial cooperation related to interception of telecommunications

6.2.2.1 The Law on the European Investigation Order

Bulgaria transposed Directive 2014/41/EU on the European Investigation Order (EIO) through the **Law on the European Investigation Order**, published in the State Gazette No. 16 on 20 February 2018. Like the Slovenian Act on Cooperation in Criminal Matters with Member States of the EU, the Bulgarian Law on the EIO incorporated specific provisions on telecommunication interception (Articles 30 and 31) and Annexes A and C of the EIO.

In Bulgaria, the transposition of the EIO Directive faced significant challenges. Namely, *the original text of the law did not provide for legal remedies against the issuance of an EIO or the execution of coercive investigative measures during the investigative phase*. This absence of legal recourse was highlighted in the case of 'Ivan Gavanozov II' (C-852/19), where the Court of Justice of the European Union (CJEU) ruled on 11 November 2021 that Bulgaria's lack of legal remedies infringed upon fundamental rights as enshrined in the EU Charter of Fundamental Rights. Consequently, *the CJEU determined that, under such circumstances, Bulgaria was precluded from issuing EIOs until appropriate legal remedies were established. to comply with EU standards*. **The amended Law, which is currently in place, aligns with the Directive's requirements, ensuring that requests for measures are processed in accordance with the standardised forms and procedures outlined in the Directive.**

6.2.2.2 Issuing and executing EIOs in cases involving telecommunications interception

In the amended Article 5(1)(1) of the Law on the EIO, the authority responsible for issuing and executing an EIO is designated in accordance with Article 2(c) of Directive 2014/41/EU. The competent authorities are:

(a) Issuing authority:

- Public prosecutor – The public prosecutor is the primary authority competent to issue an EIO during the pre-trial phase of criminal proceedings (Article 5(1)(1) of the Law on the European Investigation Order).
- Court – During the trial phase, the competent court handling the case can issue an EIO.

(b) Executing authority:

- Bulgarian court – If the execution of the EIO requires judicial authorisation (e.g., coercive measures such as house searches, wiretapping, or surveillance), the court must approve and oversee its implementation.

- Prosecutor's office – The prosecutor is responsible for ensuring the execution of the EIO, particularly for non-coercive measures and for coordinating with law enforcement agencies.
- Ministry of Justice – Acts as a central authority for administrative assistance and coordination in cross-border cases when necessary.

If the EIO relates to real-time interception of telecommunications, the request must be approved by a Bulgarian court. The competent court typically reviews such requests to ensure they comply with national legal standards.

The recognition or execution of an EIO may be refused on several grounds set out in the Law on the EIO and Article 11 of Directive 2014/41/EU, including concerns related to fundamental rights, lack of dual criminality, national security interests, or the absence of required judicial authorisation, among others.

6.2.2.3 EIO statistics

According to the 2023 activity report of the Prosecutor's Office of the Republic of Bulgaria, a total of 1,028 EIOs were received for execution (compared to 1,034 and 1,024 in the previous two years, respectively). Meanwhile, 1,477 EIOs were issued by first-instance prosecutor's offices (up from 1,238 in 2022 and 1,254 in 2021), representing an increase of 19.3% compared to 2022 and 17.8% compared to 2021. These numbers indicate that over the past three years, there has been a clear upward trend in outgoing EIOs and fluctuating volumes of incoming EIOs, indicating that this instrument is actively used by both the Bulgarian prosecutor's office and competent authorities in other EU Member States.

Table 5: Number of outgoing EIOs (Bulgaria)
Source: The Prosecution office – annual reports for the 2019-2024 period (https://prb.bg/bg/pub_info/dokladi-i-analizi)

	2024	**2023**	**2022**	**2021**	**2020**	**2019**
MLAR	487	494	395	373	331	602
EAW	234	190	143	153	221	239
EIO	1675	1477	1238	1254	981	846

Table 6: Number of incoming EIOs (Bulgaria)
Source: The Prosecution office – annual reports for the 2019-2024 period (https://prb.bg/bg/pub_info/dokladi-i-analizi)

	2024	**2023**	**2022**	**2021**	**2020**	**2019**
MLAR	1843	1449	894	1081	1252	1636
EAW	244	229	240	248	202	189

EIO	956	1028	1034	1024	843	807

The Bulgarian project partner notes that it remains unclear whether the Prosecutor's Office provides data on the total number of European Investigation Orders (EIOs) or only on those issued or received specifically by the prosecution, given that Article 5(1) of the Law on the EIO designates multiple authorities as competent for issuing and executing EIOs.

Although the obligation for the prosecution to collect and publish annual statistics on EIOs has been in force since 2019, only general figures are publicly available in Bulgaria. For instance, there is no specific data on how many incoming EIOs – received from other Member States – have been accepted (and executed) or rejected by Bulgarian authorities. Similarly, there is no data on outgoing EIOs that were accepted or rejected by the authorities of other Member States.

Another important limitation concerning EIO statistics is that, while the available data reflects the overall use of EIOs for various types of cross-border investigative measures, it does not provide a breakdown by specific types of measures, and in particular, not for covert investigative measures. In other words, in Bulgaria, official data on covert investigative measures in general, and telecommunications interception in particular, is not publicly accessible – a situation that, as previously noted, also applies to Slovenia.

6.3. The Czech Republic

6.3.1 Provisions on the interception of telecommunications

6.3.1.1 Overview of the legal framework

In the Czech Republic, covert investigative measures (CIM), including real-time interception of telecommunications, are primarily governed by **Act No. 141/1961 Coll., on Criminal Judicial Procedure** (the 'Criminal Procedure Code').[188] This legislation establishes the prerequisites for wiretapping and other forms of interception, requiring judicial authorisation and strict adherence to the principles of necessity and proportionality. Judges must ensure that such intrusions into privacy are justified only in serious criminal cases, and only when less intrusive means are insufficient.

CIM can be routinely implemented by law enforcement authorities within the framework of criminal procedure. However, as in Bulgaria and unlike in Slovenia, in criminal investigations, the mandate to use CIM is also granted to intelligence agencies. The activities of the intelligence community are governed by **Act No. 153/1994 Coll., on Intelligence Services of the Czech Republic**,[189] **Act No. 154/1994 Coll., on the Security Information Service**,[190] and **Act No. 289/2005 Coll., on Military Intelligence**.[191] These laws define which national security bodies are authorised to use telecommunications interception tools, under what conditions, and subject to what forms of specialised judicial oversight.

[188] Czech Republic: Act No 141/1961 https://www.e-sbirka.cz/sb/1961/141/2025-02-11?f=141%2F1961&zalozka=text accessed 31 July 2025.
[189] Czech Republic: Act No 153/1994 https://www.e-sbirka.cz/sb/1994/153/2025-01-01?f=153%2F1994&zalozka=text accessed 31 July 2025.
[190] Act No 154/1994 (Czech Republic) https://www.e-sbirka.cz/sb/1994/154/2019-09-06?f=154%2F1994&zalozka=text accessed 2 August 2025.
[191] Act No 289/2005 (Czech Republic) https://www.e-sbirka.cz/sb/2005/289/2021-07-01?f=289%2F2005&zalozka=text accessed 2 August 2025.

Cooperation obligations for telecommunication services are introduced by **Act No. 127/2005 Coll., on Electronic Communications,**[192] which requires providers to enable lawful interception while also mandating strict conditions to protect user confidentiality. Specific rules and requirements are included in the implementing legislation to the Act on electronic communications.

6.3.1.2 Covert investigative measures related to communications interception

Under Czech law, three key covert investigative measures relate to the interception of telecommunications.

First, **wiretapping or interception of electronic communications**, governed by § 88 of the Criminal Procedure Code, allows law enforcement authorities to carry out real-time interception of telecommunications traffic – such as phone calls and electronic messages – subject to a judicial warrant and a strict necessity and proportionality test.

Second, **access to stored communications metadata**, regulated by § 88a of the Criminal Procedure Code, enables investigators to obtain metadata retained for up to six months by internet service providers, in accordance with data retention obligations set out in the Act on Electronic Communications.

Third, **surveillance of persons and objects**, pursuant to § 158d of the Criminal Procedure Code, encompasses a range of investigative techniques, including access to stored communication content that may be relevant to an ongoing investigation.

Additionally, the Criminal Procedure Code permits **the freezing of stored data** under § 7b, ensuring that critical electronic evidence remains preserved for the duration of criminal proceedings.

Although the law explicitly defines key covert investigative measures, it does not specifically address the use of technologies such as **IMSI catchers** or **Trojan horse software**. However, these methods are not explicitly prohibited and may be employed if they fall within the legal scope of existing investigative powers and are authorised by a relevant judicial decision.

In practice, courts and law enforcement authorities interpret such advanced tools as permissible extensions of legally sanctioned interception or surveillance measures – provided that the **principles of necessity and proportionality** are respected and a valid judicial warrant is obtained.

The Criminal Procedure Code refers to **telecommunications interception** (*odposlech a záznam telekomunikačního provozu*) primarily in § 88, which requires a *court order* authorising the *real-time monitoring of conversations* or the *ongoing transmission of data*. This provision applies to specific categories of criminal investigations, typically involving *offences with higher statutory penalties or elements of organised crime*.

Access to stored communication metadata under § 88a is subject to a similar requirement for *judicial authorisation*, allowing law enforcement to obtain previously retained call logs and connection details.

[192] Act No 127/2005 (Czech Republic) https://www.e-sbirka.cz/sb/2005/127/2025-01-01?f=127%2F2005&zalozka=text accessed 2 August 2025.

Meanwhile, **surveillance** (*sledování osob a věcí*), governed by § 158d, permits the monitoring of individuals and objects, including the collection of stored communication content, if it is necessary to clarify facts relevant to a criminal proceeding.

6.3.1.3 Categories of intercepted or accessed data and conditions for the interception

More specifically, the Czech Criminal Procedure Code distinguishes between several categories of intercepted or accessed data, each subject to specific prerequisites and conditions:

- **Real-time interception of communication content** (§ 88): Also referred to as wiretapping, this measure allows authorised authorities to listen to or record ongoing calls or data transmissions. A court order is mandatory, and the request must demonstrate the seriousness of the offence, the insufficiency of alternative investigative tools, and strict compliance with the principle of proportionality.
- **Historical metadata of previously conducted communications** (§ 88a): In addition to live interception, § 88a governs access to metadata – such as call logs and connection details – relating to past communications. Although based on the same legal foundation as real-time interception, the evidentiary standards and justification required may differ slightly, depending on the nature and purpose of the data being sought.
- **Stored content of previously conducted communications** (§ 158d): Under the provisions on the surveillance of persons and objects, investigators may access stored digital content (e.g., previously exchanged messages) if doing so is essential to clarify facts relevant to a criminal proceeding. Judicial authorisation is required, and the measure must be proportionate to the seriousness of the offence.
- **Freezing of stored data** (§ 7b): The Code also allows for the freezing of stored data to prevent its destruction or alteration, thereby preserving evidence crucial to ongoing criminal proceedings.

The legal prerequisites for implementing such measures require showing that: (1) a criminal offence of sufficient gravity is under investigation; (2) existing evidence-gathering methods are inadequate; (3) the proposed measure is proportionate to the seriousness of the offence; and (4) a competent court has issued or approved the necessary authorisation. These measures are typically subject to strict time limits and must be accompanied by detailed documentation of their execution.

6.3.1.4 Time limitations, procedural safeguards, admissibility, remedies, and oversight

Regarding the *interception of electronic communications* (§ 88), courts generally authorise wiretapping for a limited initial period – typically a few weeks to several months, up to a maximum of four months per order. Renewals may be granted if the statutory prerequisites of necessity and proportionality continue to be met. While there is no specific limit on the number of renewals, each extension must not exceed four months. Once the authorised timeframe expires, or if the interception no longer serves an investigative purpose, law enforcement must immediately cease the measure.

Evidence obtained through intercepted communications may be presented in criminal proceedings, provided the interception was lawfully authorised and the material is relevant to the case. Evidence obtained by telecommunication interception is subject to strict procedural safeguards to ensure its legality and reliability. Pursuant to the Criminal Procedure Code, any real-time interception of communications (or access to stored content) requires a judicial warrant and must be carried out in accordance with the principles of necessity and proportionality. If these requirements are not met – such as when interception is conducted without proper authorisation

– the resulting evidence is generally deemed inadmissible under §89(3) of the Criminal Procedure Code. Courts also have the power to examine the circumstances of how evidence was obtained and to disallow evidence that violates procedural safeguards or constitutional rights. Any data found to be unrelated to the offence under investigation must be either destroyed or secured in a manner that prevents unauthorised access.

A different framework applies to *access to stored communications metadata* (§ 88a), which involves retrieving call logs, connection records, and other data retained by service providers. Although subject to the same principles of necessity and proportionality, authorisation under § 88a typically permits one-time access to historical metadata. The retention period for such records is governed by the Act on Electronic Communications, which limits the storage of metadata to up to six months.

Surveillance of persons and objects (§ 158d), which may include accessing stored communication content relevant to an investigation, is subject to strict judicial oversight and clearly defined timeframes. The police may conduct surveillance only for the duration specified in the court order, which may last up to six months. Surveillance must cease immediately when the order expires or when the measure becomes unnecessary. Extensions may be granted if the statutory conditions of necessity and proportionality are still fulfilled; again, there is no fixed limit on the number of renewals, but each may last no longer than six months. Although information obtained through surveillance may be used as evidence, it must be shown to have been lawfully acquired within the authorised timeframe and scope. Evidence obtained outside these parameters must be excluded or destroyed.

Finally, *freezing of stored data* (§ 7b) is a measure intended to preserve electronic evidence that is likely to be significant in criminal proceedings. A freezing order temporarily suspends the deletion or alteration of specified data for a period of up to 90 days, allowing investigators time to obtain the evidence through proper legal channels. While 'frozen' data cannot be used directly as evidence until formally accessed, the measure helps prevent the loss or tampering of potentially critical information. Once the data is no longer needed for the criminal procedure – or if a court finds the freezing order unjustified – it must be lifted without undue delay.

Across all four measures, Czech law imposes *continuous oversight* to ensure that any authorisation remains both necessary and proportionate. Judicial approval, which is required at the outset, may be extended only with proper justification, and must be terminated as soon as the objectives have been achieved or the authorised time limit expires. Persons whose communications have been intercepted without due process can challenge the lawfulness of the interception either during pre-trial proceedings (by *filing a complaint against the conduct of law enforcement or a motion to exclude the unlawfully obtained evidence*) or at trial (by *contesting the admissibility of the evidence before the court*). Moreover, if no effective relief is granted at the trial or appellate level, the affected individual can lodge a *constitutional complaint* (*ústavní stížnost*) with the Constitutional Court, alleging a breach of their fundamental rights.

6.3.1.5 Constitutional review of the Electronic Communications Act and the Special Surveillance Means Act provisions related to telecommunications interception

The Czech Constitutional Court has extensively reviewed the normative framework for telecommunication interception, clarifying both procedural requirements and constitutional boundaries.

Earlier rulings, such as **ÚS 22/1993 (II. ÚS 6/93)**, already questioned the use of wiretap evidence in subsequent proceedings, though the Court's observations there were later clarified by legislative amendments (notably in § 88(6) of the Criminal Procedure Code) specifying when intercepted material may be reused in a different case. Moreover, in **ÚS 78/1995 (III. ÚS 62/95),** the Court held that communications between attorneys and their clients enjoy particularly robust protection and cannot be subject to lawful interception. This theme of privileged communications reappears throughout constitutional case law, requiring any accidentally captured privileged content to be segregated and destroyed.

Subsequent decisions – including **ÚS 88/2007 (II. ÚS 615/06)**, **ÚS 46/2008 (I. ÚS 3038/07)**, **ÚS 15/2010 (II. ÚS 2806/08)**, and **ÚS 152/2010 (IV. ÚS 1556/07)** – emphasise that wiretapping constitutes a grave intrusion into the right to privacy and is permissible only for statutorily defined serious crimes, supported by a detailed, individualised justification showing that milder investigative methods would be insufficient. These rulings also affirm that judicial warrants must explicitly identify the suspect using or owning the intercepted line, explain the factual basis for suspicion, and outline the anticipated evidentiary benefit. Finally, the Court has consistently stressed that any interception measure lacking concrete indicia of criminal conduct violates the principle of necessity and renders the gathered evidence unconstitutional and inadmissible.

In **Pl. ÚS 24/11**, the Court focused on data retention under the Act on Electronic Communications, and relevant provisions of the Criminal Procedure Code. It found certain rules disproportionate for allowing indiscriminate and broad retention of telecommunications data without adequate safeguards, thus invalidating them as unconstitutional. Parliament responded by refining the legislation, imposing stricter time limits, reinforcing proportionality reviews, and enhancing judicial oversight.

Additionally, in **Pl. ÚS 47/13**, the Court once again scrutinised statutory provisions enabling broad access to telecommunications data. Building on its earlier rulings, it reinforced that any intrusion into constitutionally protected privacy rights must be narrowly tailored and demonstrably necessary for specific criminal investigations. The decision underscored the imperative of precise legislative safeguards and effective judicial control to prevent disproportionate surveillance or misuse of retained data, thereby further consolidating the stringent requirements already established by the Constitutional Court's case law.

Overall, these constitutional reviews have shaped a more rigorous legal environment for telecommunication interception, obligating courts and law enforcement to demonstrate why a wiretap is essential, to limit its scope and duration, and to protect privileged or irrelevant communications. Failure to fulfil these conditions can result in exclusion of the evidence and, in certain cases, orders to destroy all improperly obtained records.

6.3.2 Provisions on cross-border judicial cooperation related to interception of telecommunications

6.3.2.1 Act on International Judicial Cooperation in Criminal Matters

Directive 2014/41/EU on the EIO has been transposed primarily through **Act No. 104/2013 Coll., on International Judicial Cooperation in Criminal Matters**,[193] which was updated to integrate the EIO regime into national law. Part 2 of this Act establishes procedures enabling Czech

[193] Act No 104/2013 (Czech Republic) https://www.e-sbirka.cz/sb/2013/104/2025-01-01?f=104%2F2013&zalozka=text accessed 2 August 2025.

authorities both to issue outgoing EIOs for evidence gathering in other EU Member States and to recognise and execute incoming EIOs received from abroad. While Czech implementation largely mirrors the Directive's provisions, a key feature is the linkage between the EIO framework and the existing national rules in the Criminal Procedure Code for authorising and overseeing CIV.

6.3.2.2 Issuing and executing EIOs in cases involving covered investigative measures, including telecommunications interception

With regard to telecommunication interception requests, the Act follows the templates and procedural steps outlined in Annex A (Request for the issuing of an EIO) and Annex C (Additional information related to telecommunication interception) of the Directive, ensuring that Czech authorities comply with standardised forms and safeguard measures.

Outgoing EIOs

Act on International Judicial Cooperation in Criminal Matters designates both the **presiding judge** (*předseda senátu*) and the **public prosecutor** (*státní zástupce*) as the principal authorities for issuing an outgoing EIO, depending on the procedural stage. During the pre-trial phase, it is generally the public prosecutor who issues the EIO to obtain evidence abroad. However, *if the investigative measure in question requires judicial authorisation under Czech law* (for instance, measures that only a judge can permit), the judge must confirm the EIO upon a reasoned request from the public prosecutor. In doing so, the *judge reviews the necessity and proportionality of the proposed measure* and ensures it aligns with the legal prerequisites for a comparable domestic case.

Once an indictment has been filed, the *authority to issue an EIO typically shifts to the presiding judge*. Nevertheless, the law allows the public prosecutor to issue an EIO after an indictment has been submitted if the evidence in question is necessary for representing the prosecution before the court. This requires a similar judicial confirmation if the measure sought would ordinarily fall within the judge's exclusive competence. Through this framework, the *Czech system ensures that EIOs comply with the same legal safeguards – particularly those regarding necessity, proportionality, and judicial oversight – that apply to purely domestic investigative measures*.

Incoming EIOs

The authority responsible for executing a EIO or other requests for legal assistance depends on the *procedural stage of the foreign criminal proceedings* and the *nature of the requested measure*. If the requesting state is conducting a pre-trial investigation, the Regional Public Prosecutor's Office (*krajské státní zastupitelství*) with territorial jurisdiction over the location where the requested measure must be carried out is typically competent. However, where the requested measure requires judicial authorisation under Czech law, the Regional Court (*krajský soud*) may also be involved. In instances where multiple offices or courts could be competent, the Supreme Public Prosecutor's Office (*Nejvyšší státní zastupitelství*) or the Ministry of Justice (*ministerstvo spravedlnosti*) may determine which authority will handle the request, or direct communication rules may apply so that the authority first receiving the request proceeds with it.

When the measure involves certain intrusive or otherwise judicially overseen acts, it is commonly the District Court (*okresní soud*) located in the seat of the competent Regional Court that carries out these tasks. Specific provisions detail which district court corresponds to each region (for instance, in Prague, it is generally the District Court for Prague 1). Additionally, authorities may exercise territorial flexibility to expedite or simplify the execution of requests, such as performing an investigative measure outside their usual district in urgent cases or delegating a simpler legal

assistance task to a lower-tier authority. This tiered framework mirrors the system for purely domestic measures, ensuring that *foreign requests, including EIOs, follow the same procedural safeguards and division of responsibilities that apply in Czech criminal proceedings*.

Under the Act on International Judicial Cooperation in Criminal Matters, requests for CIM, including telecommunications interception, submitted via an EIO must undergo a process akin to that used for purely domestic authorisations, ensuring they meet the same legal prerequisites and safeguards required by Czech law. If an EIO requests an investigative measure that would normally require a warrant or judicial authorisation in the Czech Republic - such as wiretapping or surveillance - it can only be executed once a competent Czech authority (usually a court) has confirmed that the measure is both necessary and proportionate under domestic standards. The Regional Public Prosecutor's Office (or Regional Court, if a judge's order is required) will assess the EIO, verify its compliance with Czech procedural rules, and then either implement the request itself or pass it on to the District Court with territorial jurisdiction over the place where the measure must be carried out.

Grounds for refusal determined by Article 11 of Directive 2014/41/EU are reflected in (§365) of the Czech Act on International Judicial Cooperation in Criminal Matters. In practice, however, EIO requests for covert investigative measures are not refused lightly. Courts and prosecutors typically seek to accommodate them unless a clear legal barrier arises. The resulting evidence, once lawfully gathered, is admissible in the requesting Member State's criminal proceedings under the rules of the EIO framework, though Czech authorities must ensure it was obtained in accordance with domestic procedural standards.

6.3.2.3 EIO statistics

Regarding statistical data on the frequency of EIO use, *official figures on covert investigative measures specifically are not published in detail.* However, aggregated data from the Ministry of Justice and Supreme Public Prosecutor's Office[194] suggest **an overall increase in requests for international cooperation (including EIO) in recent years**, mirroring trends across the European Union. While comprehensive statistics differentiating covert measures from other types of investigative assistance are limited, practitioners report that *requests for surveillance, interception, or similar actions constitute only a subset of total EIO applications* – most of which relate to simpler measures such as taking witness testimony or gathering documentary evidence. Nevertheless, the growing familiarity with the EIO mechanism among prosecutors and courts has steadily expanded the number of cross-border investigative requests, including those involving covert techniques.

6.4. Poland

6.4.1 Provisions on the interception of telecommunications

6.4.1.1 Overview of the legal framework

In the Polish legal system, the legal framework governing the interception of telecommunications is fundamentally grounded in the **Constitution** and the rights and freedoms it guarantees. Of particular relevance are Articles 47 and 49, which protect *private and family life*, *honour and good name*, as well as the *freedom and secrecy of communications*. These rights may only be restricted

[194] Czech Republic: Office of the Public Prosecutor https://verejnazaloba.cz/nsz/cinnost-nejvyssiho-statniho-zastupitelstvi/zpravy-o-cinnosti/ accessed 31 July 2025.

in cases explicitly provided by law and in a manner prescribed therein. Any restrictions on constitutional freedoms and rights must not infringe upon their essence (Article 31(3) of the Constitution). Also noteworthy is Article 51(2), which stipulates that public authorities are prohibited from obtaining, collecting, or sharing information about citizens beyond what is necessary in a democratic state governed by the rule of law.

Covert investigative measures involving telecommunications interception are governed by the provisions of the **Act of 6 June 1997 – Code of Criminal Procedure (CCP)** and several other statutes:

- Chapter 26 of the Act of 6 June 1997 – CCP, and Article 168b of that Code;
- Article 19(1)(1–9) of the **Act of 6 April 1990 on the Police**, which allows wiretapping in a closed catalogue of specified cases;
- Article 27(6) of the **Act of 24 May 2002 on the Internal Security Agency and the Foreign Intelligence Agency**, which grants the Internal Security Agency authority to conduct operational surveillance;
- Article 11n(1–2) of the **Act of 21 June 1996 on Certain Powers of Employees of the Ministry of Internal Affairs and Officers and Employees of Agencies Supervised by that Minister**, which enables operational control in the form of wiretapping for officers of the Police, Border Guard, and State Protection Service, as well as for firefighters in the State Fire Service and employees of those services;
- Article 17(5) of the **Act of 9 June 2006 on the Central Anti-Corruption Bureau**, which authorises the Bureau to carry out surveillance targeting specific persons or particular acts;
- Article 118(4) of the Act of 16 November 2016 on the National Revenue Administration, which permits wiretapping in cases of fiscal offences, economic crimes, property offences, and corruption-related offences, including those committed by public officials;
- Article 31 of the **Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service**, which authorises wiretapping to detect, prevent, and investigate offences committed by active-duty soldiers, officers of the SKW and SWW, and employees of the Polish Armed Forces and other units under the Ministry of National Defence – particularly crimes against peace, humanity, and war crimes;
- Article 42(3) of the **Act of 8 December 2017 on the State Protection Service**, which permits wiretapping in connection with criminal offences explicitly enumerated in the provision;
- Article 9e of the **Act of 12 October 1990 on the Border Guard**;
- Article 31 of the **Act of 24 August 2001 on the Military Gendarmerie and Military Law Enforcement Authorities**;

Under the Polish law, two parallel systems of applying covert investigative measures including telecommunication interception exist: (a) the procedural system, regulated by the CCP, where interception is ordered by a court at the request of a prosecutor during the preparatory proceedings; and (b) the extraprocedural (e.g., operational) system, regulated by special statutes, where interception is ordered by a court at the request of the police or another law enforcement authority, with the prosecutor's prior consent, typically before the initiation of preparatory proceedings.

Notably, Polish legislation does not explicitly use the terms *'covert investigative measures'* and *'interception'* in its statutory provisions, despite their frequent use in legal and political discourse. Different statutes use varying terminology for covert investigative measures. The same applies to interception: while the CCP refers to it as 'surveillance and recording of the content of telephone conversations' or simply 'surveillance and recording of conversations,'[195] the other statutes mentioned above employ terms such as 'operational control,' 'use of technical means,' or 'operational wiretapping.'
According to prevailing scholarly opinion, 'interception' refers to the covert acquisition and recording of the content of communications conducted via telecommunication means, using any form of technical device. It also includes the monitoring of conversations occurring outside telecommunication systems, provided that the individual conducting the monitoring is not a participant in the intercepted communication.

6.4.1.2 Categories of covert investigative measures related to communications interception

Polish legislation provides for three main types of covert investigative measures related to telecommunications interception:
(1) Obtaining and recording the content of conversations conducted using technical means, including telecommunications networks;
(2) Obtaining and recording the content of correspondence, including correspondence transmitted via electronic communication;
(3) Obtaining and recording data contained in data storage media, telecommunications terminal devices, as well as IT and ICT systems.

The legislation does not further specify the details of these measures. Each may be applied only under *strictly defined circumstances* and is *limited to a closed catalogue of offences* outlined in the CCP and specific statutes (see below).

With respect to the second type of covert measure, it is important to note that Polish legislation allows for the monitoring of correspondence and postal items, as well as telecommunications networks operated by all providers – regardless of ownership structure or the technology used. This includes, among others, communications transmitted via SMS, MMS, fax, email, telecommunications lines, radio, and the Internet.

No electronic device or specific method of conversation is excluded *a priori* from potential surveillance. For example, real-time exchanges of emails – such as those in the form of 'chat' messages – are considered a form of conversation, and therefore subject to the legal provisions governing telecommunications interception. However, this interpretation is not explicitly codified in binding legislation.[196]

[195] The phrase used by the Polish legislator '*kontrola i utrwalanie treści rozmów telefonicznych*' is translated in EU documents as '*surveillance and recording of the contents of telephone conversations.*'

[196] See Rogalski M, *Procedural and Extraprocedural Wiretapping: Control and Recording of Conversations Based on the Code of Criminal Procedure and Special Acts* (Wolters Kluwer Polska, Warsaw 2019); Zakrzewski R and Jarocha W, *Admissibility of Correspondence Control and Wiretapping* [*Kontrola Państwowa* (State Control)] (1997); Dudka K, 'Private and Journalistic Wiretapping and Criminal Procedure' in I Nowikowski (ed), *Problems of Judicial Law Application. A Festschrift for Professor Edward Skrętowicz* (Lublin 2007).

As for the third category, it permits the acquisition and recording only of data stored on the device itself; it does not extend to surrounding audio or video captured by the phone, nor does it apply to data stored in the cloud.[197]

While the measures listed above are provided for in each of the special statutes authorising telecommunications interception, Polish *legislation does not precisely specify the methods by which covert surveillance – including telecommunications interception – is to be conducted*; that is, there is no exhaustive list of permissible technical means. Although **IMSI catchers** are not explicitly regulated under Polish law, their use appears to be permitted as a form of 'technical means' authorised under specific
statutes, provided they operate passively and do not alter the content of communications. In contrast, the use of '**Trojan horse'** software lacks a clear legal basis in Polish legislation.[198]

Notwithstanding the absence of explicitly stated restrictions on the technical means that may be used for the interception of telecommunications, *their use must comply with the constitutional framework.* In **Judgment of 30 July 2014, case no. K 23/11**, the Constitutional Tribunal held that, to uphold constitutional guarantees, it is sufficient to interpret the law as requiring the authority ordering covert surveillance to specify the technical means to be used in each individual case. From a constitutional standpoint, only those technical means that are provided for by law and may be used by the authority applying for the surveillance order are permissible. The authorities must particularly consider the need to apply only proportionate measures and to respect fundamental rights, such as the right to privacy, the confidentiality of correspondence, and human dignity – core principles in a democratic state governed by the rule of law.

In addition to the absence of a clear determination of which specific forms and tools may or may not be used, the *legislator has also failed to specify the elements that a court order authorising operational control through surveillance (e.g., interception) should contain*.

6.4.1.3 Procedure and prerequisites for the interception of telecommunications

Under the Polish law, the procedures and legal requirements for conducting covert operational activities, including telecommunications interception, vary depending on whether the interception is carried out under the CCP or under specific legislative acts (the so-called 'special acts' mentioned above). Under the provisions of the CCP, a *justified suspicion* that a specific (catalogued) offence was committed (Article 237 § 3 of the CCP) or a *justified concern* regarding the commission of a new specific offence, and the purpose of detecting and obtaining evidence is necessary to initiate preparatory proceedings by a *judicial warrant*. Under special legislative acts, a written consent of the Prosecutor General should be obtained by the police or other LEAs to initiate proceedings by a *judicial warrant*. Other prerequisites include:

[197] See Opitek P, 'Operational Control of End Devices' (*Prokuratura i Prawo* [*Prosecution and Law*] issue 4, 2023).
[198] While it appears that Polish security services are in possession of such software, under the currently binding law Trojan horse software should not be used. None of the statutes provide for the admissibility of taking control over a device or modifying the data stored in its memory. The only exception is Article 32a(7) of the Act on the Internal Security Agency and the Intelligence Agency. According to provisions of this article, only the Internal Security Agency (ABW) is authorised to use this type of software but solely for a narrowly defined and strictly specified purposes outside the scope of operational control, (e.g., outside the scope of telecommunications surveillance).

(a) the ineffectiveness or inadequacy of other means of conducting operational and investigative activities;
(b) submission by the competent authority of an application to the appropriate court for authorisation of the activity;
(c) inclusion in the application of evidence substantiating the necessity of operational control;
(d) execution of operational control for a statutory purpose and within the scope of a closed list of specified offences;
(e) pursuit of objectives such as the identification, prevention, and detection of offences listed in the special acts, as well as the identification of perpetrators and the collection and preservation of evidence;

Each of the special statutes contains its own catalogue of offences authorizing the use of surveillance of telecommunications, which differs from the one provided in the CCP. Moreover, in the context of those statutes, it is additionally emphasized that there is no doubt that operational control may be employed regardless of whether criminal proceedings are already underway (both in the *in rem* and *in personam* phases) or not.

Telecommunications interception conducted by agencies or entities other than the police - such as the Border Guard, Military Gendarmerie, Central Anti-Corruption Bureau, National Revenue Administration, and Internal Security Agency - may be ordered, and the materials they obtain may be used in criminal investigations, only when it is *necessary in the interest of justice* and when the *relevant facts cannot be established by any other means of evidence*. The decision to include such evidence is made by the court upon the prosecutor's request.[199]

Statutory provisions do not explicitly articulate the ***principle of proportionality***. Nevertheless, in the Polish legal doctrine, it is universally accepted that, given the significant restrictions imposed on constitutionally guaranteed rights and freedoms, the interception and recording of telephone conversations and other forms of telecommunications may only be ordered when such measures are *necessary* and *proportionate*. In other words, telecommunications interception must serve a clearly defined statutory purpose. It must also be necessary – meaning essential for resolving the matter under investigation – and proportionate, that is, commensurate with the level of interference with constitutionally protected rights and freedoms.

The Polish Constitutional Tribunal has repeatedly addressed the principle of proportionality in the context of restricting individual rights. It has emphasised that '*it is not sufficient for the measures employed merely to facilitate the achievement of intended objectives, make their attainment easier, or prove convenient for the authority applying them. Such measures must be worthy of a state described as democratic and governed by the rule of law. Moreover, in a democratic state governed by the rule of law, it is never permissible to retain information obtained covertly merely because it may prove potentially useful, without any connection to ongoing proceedings*.' According to the Tribunal, interception and recording of communications should be carried out exclusively for the purpose of obtaining essential evidence that is significantly relevant to ongoing proceedings or to prevent the commission of a serious offence. Telephone interception should not be ordered simply to collect arbitrary or speculative evidence. This principle is also reflected in the statutory requirement under the special acts, which stipulates that covert surveillance may

[199] Entities such as the Border Guard, Military Gendarmerie, Central Anti-Corruption Bureau, National Revenue Administration, and Internal Security Agency possess, within the scope of their statutory competences, investigative powers equivalent to those of the Police in the context of criminal proceedings. In the Polish law, these agencies are referred to as other formations authorized to participate in the criminal process.

be used only if other evidentiary measures have proven ineffective or are unsuitable (Constitutional Tribunal judgment of 12 December 2005, case no. K 32/04).

6.4.1.4 Time limitations

Monitoring and recording of telephone conversations (and other forms of telecommunications) may be authorised for a *maximum period of 3 months*, with the possibility of *extension – only in particularly justified cases – for an additional period of up to 3 months* (Article 238 § 1 of the CCP). A 'particularly justified case' refers to exceptional circumstances, and any extension of the interception must be supported by a clear demonstration that this condition is met.[200]

The decision to extend the duration of monitoring is issued by the court upon the prosecutor's request. The prosecutor's request for an extension of wiretapping must set out the circumstances justifying the continued necessity of the measure. The decision to extend the use of telephone tapping is made by the same court that is competent to authorise its initial use (Article 237 § 2 of the CCP).

Surveillance (e.g., the interception and recording of communications) must be terminated immediately once the reasons specified in Article 237 §§ 1-3 of the CCP no longer apply, and in any case, no later than the expiration of the period for which it was authorised (Article 238 § 2 of the CCP).

The justification for extending interception beyond the initial three-month period may be supported by the positive results obtained thus far – particularly if those results indicate that continued surveillance is likely to produce even more substantial evidence.

The time periods specified in Article 238 § 1 of the CCP do not need to be used all at once; they may be applied in instalments. Therefore, it is permissible to implement and extend the monitoring and recording of conversations multiple times, as long as the total duration does not exceed the initial three-month period and, in particularly justified cases, an additional three months. The provision uses the phrase 'a maximum of a further 3 months,' indicating that the extension may be granted for a shorter period if appropriate.

In total, **the monitoring and recording of telephone conversations within a single proceeding may not exceed 6 months**. Extensions beyond this six-month limit are not permitted, even if they are justified and deemed necessary.

In addition to the time limits specified in Article 238 § 1 of the CCP, the legislator has established a *general timeframe within which this means of evidence may be used* – namely, during the pre-trial stage, from the decision to initiate an investigation or inquiry until the decision to close the preparatory proceedings, and during court proceedings, from their commencement until their conclusion.

[200] General rules of argumentation in law suggests that if the application of a provision is only permissible in *particularly justified cases*, that provision should not be subject to a broad interpretation. This rule notwithstanding, objections have been raised to the current wording of Article 238 § 1 of the Code of Criminal Procedure. The Constitutional Tribunal has indicated that 'particularly justified cases' is an imprecise term and may lead to unjustified differences in the treatment of persons to whom this provision applies. Furthermore, excessive generality may encourage arbitrary decisions. It is not sufficiently clear when the court should grant the prosecutor's request and extend the interception of communications, in particular what circumstances require the continued use of interception. Due to the lack of precision and clarity in the definition of the term 'particularly justified case' in Article 238 § 1 of the Code of Criminal Procedure, proposals have been made to amend it.

However, in the case of operational wiretapping, its use is not strictly limited by the formal stages of preparatory or court proceedings. It may be conducted before the initiation of a trial, during its course, and even after its conclusion. As a result, operational surveillance of telephone conversations can begin well before the prosecutor decides to initiate an investigation or inquiry. Moreover, even when the prosecutor orders wiretapping under the provisions of the CCP (i.e., procedural surveillance), this does not preclude the simultaneous use of wiretapping authorised under police legislation.

Notably, there is a *fundamental difference between procedural and operational surveillance* (e.g., interception) in terms of the timing and duration of their use. Pursuant to Article 19(8) of the Police Act of 1990, operational surveillance – unlike procedural surveillance – may initially be ordered for a period not exceeding three months. However, if the reasons for the surveillance persist, the district court may extend it once for an additional three months. Paragraph 9 provides for the possibility of further extensions in justified cases, particularly when new circumstances arise during the course of operational surveillance that are relevant to preventing or detecting a crime, identifying perpetrators, or gathering evidence. This framework allows wiretapping to be adapted to the actual needs of criminal proceedings.

6.4.1.5 Procedural issues of telecommunications interception and admissibility of evidence

In Poland, legal doctrine has consistently rejected the admissibility of recordings obtained through unlawful wiretapping, regardless of whether the interception was conducted procedurally or operationally. The prevailing legal view, also reflected in constitutional discourse, emphasises that even a significant public interest cannot justify breaching the legal rules governing the collection of evidence through wiretapping. Such breaches would undermine the constitutional protection of fundamental rights and the principle of judicial oversight over intrusions into those rights.

In their report on the national normative framework concerning the admissibility of evidence obtained through telecommunications interception, colleagues from AMU particularly emphasised the *issue of admitting wiretap evidence related to individuals or acts not specified in the court order authorising the surveillance*. They highlighted that the prohibition on using material obtained from monitoring conversations involving persons not named in the court order – or relating to acts outside the scope of that order – serves as a safeguard to protect the accused from being convicted through unlawful means. This rule has a protective function, representing a compromise between the constitutionally guaranteed secrecy of communications and the pursuit of truth in criminal proceedings.

Colleagues from AMU explained that the Polish legal framework on covert measures, including surveillance of telecommunications, has been amended to expand the list of offences for which evidence obtained through the surveillance and recording of conversations may be used (new Article 237a of the CCP). This development has raised concerns among legal experts. It is noted that, based on a literal interpretation of the new provision, evidence obtained during the interception of communications could be used for other offences prosecuted ex officio – not only those enumerated in Article 237 § 3 of the CCP, but also fiscal offences. This raises important questions about the relationship between this provision and the exhaustive list of offences under Article 237 § 3, particularly since the current wording of Article 237a permits the use of intercepted evidence even for offences not included in that list.

Several legal experts have pointed out that the current wording of Article 237a of the CCP appears to conflict with Article 237 § 3 of the same Code. This discrepancy may lead to an interpretation

in which Article 237a takes precedence. Notably, there is currently no provision – such as a hypothetical Article 237 § 8 – that would explicitly state that only evidence obtained in connection with the investigation of the offences listed in Article 237 § 3 may be used. In other words, no provision currently prohibits the use of intercepted material related to offences beyond those specifically enumerated.

This legal gap raises concerns about potential arbitrariness in the covert activities of public authorities. As a result, materials obtained through the monitoring and recording of conversations may be used in cases involving offences not listed in Article 237 § 3 – despite the fact that individuals should be able to know which behaviours expose them not only to potential criminal liability but also to covert investigative measures that significantly infringe on their rights to privacy and the confidentiality of communication.

Polish legal doctrine underscores that Article 237a violates the principle of proportionality as broadly defined in Article 31(3) of the Polish Constitution. It disproportionately interferes with several constitutionally protected rights: the right to privacy (Article 47), the freedom and protection of the secrecy of communication (Article 49), the inviolability of the home (Article 50), and the prohibition against the collection of information about citizens beyond what is necessary in a democratic state governed by the rule of law (Article 51(2)).

Article 237a of the CCP currently states: '*If, as a result of surveillance, evidence is obtained indicating that the person subject to the surveillance has committed another offence prosecuted ex officio or a fiscal offence other than the one covered by the original surveillance order, or that a different person has committed such an offence, the prosecutor shall decide on the use of this evidence in criminal proceedings*.' According to insights from colleagues at AMU, the use of the phrase 'the prosecutor shall decide on the use of this evidence in criminal proceedings' raises concerns. They point out that this formulation pertains primarily to the preparatory stage of criminal proceedings, in which the prosecutor (as dominus litis) exercises control. However, the court is not bound by the prosecutor's decision to introduce such evidence and may refuse to admit it. Moreover, the current wording of Article 237a no longer requires subsequent court approval for the use of such evidence, which raises additional concerns about the adequacy of judicial oversight in protecting fundamental rights.

In the opinion of the Polish Ombudsman, the newly introduced provision – granting the prosecutor the authority to decide on the use of evidence concerning offences not included in the original catalogue or involving a person other than the one specified in the surveillance order – fails to meet constitutional standards. This legislative change violates the principle of a democratic state governed by the rule of law. Transferring the power to grant subsequent consent from the judiciary to the prosecutor does not uphold this principle, as only judicial oversight can adequately safeguard individual rights infringed by covert surveillance measures.

Furthermore, given the current legal framework regulating the functioning of the public prosecutor's office, such control cannot be considered objective or independent of executive influence. These provisions also infringe on the right to a fair trial. While the initiation of surveillance – both in procedural and non-procedural contexts – requires judicial authorisation, the subsequent use of surveillance data against a different individual now requires only prosecutorial consent, thereby weakening judicial protection.

Additionally, legal scholars emphasise that eliminating the requirement for so-called subsequent judicial consent renders inadmissible, in the main proceedings, the use of information related to an offence listed under Article 237 § 3 of the CCP if that offence was not specified in the original

court order authorising the monitoring and recording of telephone conversations. This also applies to information concerning the commission of a listed offence by a person other than the one identified in the court's surveillance order. Only a court is empowered to authorise the acquisition of information through telephone tapping. Any information obtained without such judicial authorisation – regardless of its content – is considered unlawfully obtained. Consequently, any attempt to introduce this information in the main proceedings must be rejected under Article 170 § 1(1) of the CCP, as the presentation of such evidence before the court is inadmissible.

6.4.1.6 Constitutional review of the Electronic Communications Act and the Special Surveillance Means Act provisions related to telecommunications interception

The normative framework for telecommunications interception has been extensively reviewed by the Polish Constitutional Tribunal. In its **Judgment of 30 July 2014 (ref. no. K 23/11)**, the Tribunal examined the constitutionality of the provisions contained in virtually all statutes relevant to the legal basis for covert measures. The review focused on data retention and access to telecommunications and internet data, including location data, traffic data (such as call duration, IP and email addresses), and subscriber identity.

The Constitutional Tribunal ruled that several provisions were inconsistent with the Polish Constitution due to the lack of precise regulations regarding the scope, purpose, duration, and manner of data storage and disclosure; the absence of independent judicial review or another form of oversight over the services accessing such data; and the failure to impose an obligation to inform individuals subjected to these measures after their conclusion. The Tribunal postponed the invalidation of the contested provisions for 18 months, until 6 February 2016. During this period, the legislature amended several provisions to bring them into line with constitutional standards. These amendments included the introduction of prior judicial oversight for the acquisition of correspondence content through wiretapping; the obligation to maintain telecommunications data registers; the requirement to submit annual reports to Parliament on the use of operational surveillance measures; and the specification of a closed list of offences for which such surveillance may be employed.

Judgment K 23/11 was pivotal in shaping the current legal framework for operational surveillance and the interception of communications in Poland. In response, the legislature reformed the relevant legal provisions, incorporating the principles of precision and proportionality. However, the Ombudsman's recommendations were not fully implemented – most notably, the obligation to inform individuals after the surveillance has concluded was not introduced.

In its **Judgment of 12 December 2005 (ref. no. K 32/04)**, the Constitutional Tribunal reviewed provisions of the Act on the Internal Security Agency and the Foreign Intelligence Agency. It found certain provisions to be inconsistent with the Constitution, particularly due to the absence of sufficiently detailed conditions and procedures for the use of operational surveillance by the Internal Security Agency, and the lack of a requirement for prior judicial review. In many cases, decisions were made by the prosecutor or the head of the Internal Security Agency, which the Tribunal deemed inadequate. The Tribunal postponed the repeal of the contested provisions, granting the legislature time to amend them. This ruling played a fundamental role in shaping subsequent reforms of the legal framework on operational surveillance, ultimately leading to the introduction of a judicial authorisation requirement for wiretapping and other forms of surveillance conducted by the Internal Security Agency and other services.

Another ruling by the Constitutional Tribunal **– Judgment of 7 February 2018 (ref. no. K 9/16)** – concerned the 2016 amendment to the Police Act and other statutes regulating the activities of

special services. These amendments were adopted in response to the Tribunal's 2014 judgment (K 23/11). In this case, the Ombudsman raised concerns regarding, among other issues, the retention of telecommunications data (such as billing records, location data, and IP addresses), as well as the lack of adequate safeguards for the protection of personal data, the right to privacy, and the right to be informed by individuals subjected to surveillance measures.

Although the proceedings were discontinued on formal grounds – since some of the provisions had been repealed or amended during the course of the review – the Constitutional Tribunal emphasised that the issue of protecting the right to privacy in the context of data retention remains highly relevant. The Tribunal reaffirmed the state's obligation to ensure effective and independent oversight mechanisms for authorities accessing citizens' data. It also underscored that such regulations must be proportionate and clearly defined to comply with constitutional standards, as well as with the case law of the European Court of Human Rights and the Court of Justice of the European Union (e.g., the judgment in the *Digital Rights Ireland* case).

Despite the absence of a substantive ruling, decision in K 9/16 reflected ongoing constitutional concerns regarding the proportionality of data retention and the lack of adequate safeguards for citizens. More broadly, the constitutional review highlights that the right to privacy and oversight of security services are particularly sensitive issues in Poland, underscoring the need for continuous scrutiny of the legal framework to ensure compliance with both the Constitution and European standards.

6.4.2 Provisions on cross-border judicial cooperation related to interception of telecommunications

6.4.2.1 Provisions of the Code of Criminal Procedure on EIO in cases involving communications interception

In Poland, Directive 2014/41/EU on EIO was transposed by the **Act of 10 January 2018 amending the Act – Code of Criminal Procedure** (Journal of Laws of 2018, item 201) and certain other acts. The amendment, which entered into force on 8 February 2018, introduces the following provisions on the outgoing and incoming EIO:

- Chapter 62c – Request to a Member State of the European Union to carry out investigative measures on the basis of a European Investigation Order (Articles 589w – 589zd of the CCP)
- Chapter 62d – Request by a Member State of the European Union to carry out investigative measures on the basis of a European Investigation Order (Articles 589ze – 589zt of the CCP)

In addition, three regulations have been issued by the Minister of Justice, referring to the model form and templates for an EIO and the notification of an EU Member State of the interception and recording of the content of telephone conversations which will be, are or have been carried out on its territory without technical assistance from it.

6.4.2.2 Issuing and executing EIOs in cases involving covered investigative measures, including telecommunications interception

Outgoing EIOs

A EIO may be issued during both the preparatory and court proceedings (Article 589w § 1 of the CCP). In the latter case, the competent authority is the court before which the case is pending.

During preparatory proceedings, an EIO may be issued (pursuant to Article 589w § 2 of the CCP) by:

- the prosecutor conducting the proceedings;
- the police or other authorities referred to in Article 312 of the CCP – subject to approval by the prosecutor;
- authorities authorised to conduct preparatory proceedings in criminal tax cases, as specified in Article 133 § 1 and Article 134 § 1 of the Act of 10 September 1999 – the Criminal Tax Code – are also subject to approval by the prosecutor.

An EIO may also be issued in the course of operational and reconnaissance activities (Article 589w § 7 of the CCP). In such cases, the EIO is issued by the authority conducting the activities and must be approved by the public prosecutor or the court, if the evidence sought falls within the jurisdiction of the court. The law further requires the issuing authority to consult with the executing authority in advance regarding the duration and conditions of the requested measures. These consultations aim to assess the proportionality of the request, the likelihood of successful execution abroad, and to resolve any differences in the admissibility or procedure related to operational activities.

Incoming EIOs

The authority responsible for executing an order issued by another EU Member State is the public prosecutor or the district court with jurisdiction over the location where the evidence is situated or can be obtained. In certain cases, the regional court may also have competence (Article 589ze § 1–4 of the CCP).

In the case of an incoming EIO concerning the monitoring and recording of the content of conversations, the decision to execute the order serves as a substitute for the judicial decision referred to in Article 237 of the Code of Criminal Procedure. The applicable national conditions for obtaining the type of evidence specified in the EIO determine which authority is competent to execute the order. For instance, hearings conducted under Article 185a of the CCP must be carried out by a court, as must the execution of orders for the monitoring and recording of conversations.

A question arises as to which authority – the district court or the prosecutor – is competent in cases where the measure may be ordered by either. The Code does not explicitly resolve this issue; however, Article 589ze § 2 of the CCP suggests that the court's involvement should be limited to situations in which the law expressly requires the participation of a judicial authority. In all other cases, execution of the order should therefore fall under the competence of the prosecutor.

Both the EIO Directive (Article 31) and the CCP address situations in which the identifying information of the person subject to interception (e.g. telephone number) is being used within the territory of another Member State, and the interception occurs in that State’s territory – albeit without the technical assistance of that State. In such cases, the prosecutor, the police, or the authority referred to in Article 312 of the CCP must notify the competent authority of that Member State of the intention to carry out the interception, its ongoing execution, or its completion (Article 589zd of the CCP).

6.4.2.3 EIO statistics

According to the Polish project partner, ministries do not collect detailed statistics on EIOs, including the number of orders issued and received, or their use specifically in the interception of telecommunications. However, in its publication on the European Investigation Order in judicial and prosecutorial practice, the Institute of Justice notes that Poland actively makes use of EIOs. The report analyses the practical implementation of the EIO in Poland but does not provide precise data on the total number of orders issued or received.[201]

[201] Klimczak J, Wzorek D and Zielińska E, The European Investigation Order in Judicial and Prosecutorial Practice: Identified Challenges and Development Perspectives (Institute of Justice Publishing, Warsaw 2022).

7. CASE LAW

7.1. ECtHR case law

Article 8 ECHR – Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

7.1.1 Definition of privacy

Interception of telecommunication is part of secret surveillance measures under **Article 8 ECHR** (right to privacy), whereby the ECtHR has decided on issues such as the l**egal framework** for such measures, **targeted** and **bulk interception** of telecommunication data, the **admissibility of gathered evidence** (relationship between Articles 6 and 8 ECHR), as well as the **standing of potential ECtHR applicants**. As regards the definition of privacy, it was indicated early on that the right to privacy is a multi-layered one that 'comprises also […] the right to establish and develop relationships with other human beings especially in the emotional field, for the development and fulfilment of one's own personality.'[202]

Later, the Court highlighted that it is not possible 'to attempt an exhaustive definition of the notion of 'private life,''[203] and that 'a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. […] Private life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain. It is for this reason that files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method.'[204]

It covers **physical and psychological integrity** and is not limited only to an inner circle but also includes the **right to relations with others**. It also covers the concept of reasonable expectation of privacy in regard to certain interactions with others in a non-private space.[205] It might, however, be limited by a severity test.[206] The Court has addressed in the past questions regarding victims of violence, reproductive rights, disability, end of life, data protection, police surveillance, lawyer–client relationships, surveillance of telecommunications in a criminal law context, bulk interception,

[202] X v Iceland (European Commission of Human Rights, App no 6825/74, 18 May 1976).
[203] Niemetz v Germany (ECtHR, App no 13710/88, 16 December 1992).
[204] P G and J H v United Kingdom (ECtHR, App no 44787/98, 25 September 2001) para 57.
[205] Halford v United Kingdom (ECtHR, App no 20605/92, 25 June 1997); Barbulescu v Romania (ECtHR, App no 61496/08, 5 September 2017) para 73. The concept has not developed its full potential, as it has been used mainly in the context of privacy and employment. By comparison, see *Katz v. United States*, 389 U.S. 347 (1967), where the U.S. Supreme Court, based on the concept, extended the protection of the Fourth Amendment concerning unreasonable searches and seizures.
[206] Denisov v Ukraine [GC] (ECtHR, App no 76639/11, 25 September 2018) paras 110–11, para. 110-111. The Court developed in the last years a reason-based approach and a consequence-based approach, whereby severity is used the framework of the second one.

etc.[207] Moreover, in addition to natural persons, legal persons can also be protected under Article 8 ECHR with respect to home and correspondence and thus may have the status of a victim.[208]

7.1.2 ECtHR standing of applicants regarding secret surveillance

The Court recognised a special and broad scope of standing of applicants regarding secret surveillance, whereby one does not need to be directly affected. For example, in *Iordachi*,[209] the ECtHR allowed the application of a group of fundamental rights lawyers who acted in a representative capacity in approximately fifty percent of the ECtHR Moldovan cases, and in light of past threats of criminal prosecution directed towards them.[210] In *Iliya Stefanov*,[211] the Court highlighted the necessity of a 'reasonable likelihood' that the measures were applied. In *Kennedy*,[212] it pointed to the availability of remedies and the risk of such measures being applied to the individual.

Due to certain divergences in its case-law, the theory of standing in such cases was finally elaborated in *Roman Zakharov*,[213] providing for a broad application while at the same time highlighting that no *actio popularis* exists. The Court adopted a **two-factor test**, namely: **(1) the possible application of the measure to the applicant**, and (**2) the existence of remedies**. The non-existence of remedies and the possibility of application are inversely related: the greater the lack of remedies, the less the applicant needs to show the possibility of the measure being used against him. In that regard, the Court stated:

'171. [A]n applicant can claim to be the victim of a violation occasioned by the mere existence of secret surveillance measures, or legislation permitting secret surveillance measures, if the following conditions are satisfied. Firstly, the Court will take into account the scope of the legislation permitting secret surveillance measures by examining whether the applicant can possibly be affected by it, either because he belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his communications intercepted. Secondly, the Court will take into account the availability of remedies at the national level and will adjust the degree of scrutiny depending on the effectiveness of such remedies. As the Court observed in Kennedy, where the domestic system does not afford an effective remedy to the person who suspects that he was subjected to secret surveillance, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified […] In such circumstances the threat of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential users a

[207] Council of Europe, Guide on Article 8 ECHR (28 February 2025) https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_eng accessed 2 August 2025.
[208] However, the Court afforded states a wider margin of appreciation under the proportionality assessment regarding legal persons (necessary in a democratic society). ECtHR, Bernh Larsen Holding AS and Others v Norway (ECtHR, App no 24117/08, 14 March 2013) para 106; Naumenko v Latvia (ECtHR, App no 50805/14, 23 June 2022) para 51. See also Eicke T, 'Human Rights Protection of Non-Human Subjects from the Perspective of an ECtHR Judge' EJIL: Talk! (25 April 2025); Juliussen B A, 'Monitoring, Governmental Data Access and the Invocation of Article 8 ECHR by Legal Persons' (2025) The International Journal of Human Rights (online) https://munin.uit.no/handle/10037/36407 accessed 2 August 2025.
[209] Iordachi and Others v Moldova (ECtHR, App no 25198/02, 10 February 2009).
[210] *Ibid.*, para. 31-32.
[211] Iliya Stefanov v Bulgaria (ECtHR, App no 65755/01, 22 May 2008) para 49.
[212] Kennedy v United Kingdom (ECtHR, App no 26839/05, 18 May 2010) para 124, regarding the assessment of availability of any remedies at the national level and the risk of secret surveillance measures being applied to the applicant.
[213] Roman Zakharov v Russia [GC] (ECtHR, App no 47143/06, 4 December 2015).

direct interference with the right guaranteed by Article 8. There is therefore a greater need for scrutiny by the Court, and an exception to the rule denying individuals the right to challenge a law in abstracto is justified. In such cases the individual does not need to demonstrate the existence of any risk that secret surveillance measures were applied to him. By contrast, if the national system provides for effective remedies, a widespread suspicion of abuse is more difficult to justify. In such cases, the individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures only if he is able to show that, due to his personal situation, he is potentially at risk of being subjected to such measures.'[214]

Hence, there must be awareness on the part of the legislator, as well as the bodies providing input on surveillance or interception legislation (e.g., judges, prosecutors, law enforcement), that **a much broader range of persons could challenge any problems with surveillance/interception legislation** (see factor one of the tri-partite test below), even if no measure was applied or confirmed to have been applied to a specific individual.

In recent case-law, the ECtHR took the position that **several tens of thousands of users** operating in a closed network (e.g., EncroChat) constituted **a defined group**.[215] However, ECtHR applicants are not required to confirm their participation if doing so would result in self-incrimination, thereby disproportionately affecting the effective exercise of the right to individual petition.[216] At the same time, the Court required **exhaustion of remedies in the executing State in the case of a European Investigation Order (EIO)**, referring to the CJEU's decision in EncroChat (e.g., n no check of the lawfulness of the measure in the executing State by the issuing State).[217]

7.1.3 Article 8 ECHR tri-partite test

The classical Article 8 ECHR test is a tri-partite test referring to the following:

1. **Surveillance legislation must be in accordance with the law**:

(a) There must be a basis in domestic law (whether written or unwritten);
(b) The quality of the law must be satisfactory, meaning (ba) accessibility, (bb) foreseeability of consequences, and (bc) protection against arbitrariness.[218]

2. **Pursuing one or more of the following legitimate aims**: National security, public safety, the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, and the protection of the rights and freedoms of others.

[214] *Ibid.*, para. 171. See also the recent application of this test in Ekimdzhiev and Others v Bulgaria (ECtHR, App no 70078/12, 11 January 2022), para. 264-275, regarding the lack of an effective remedy to dispel public suspicion about the abuse of secret surveillance powers, damages were available only to individuals who had been notified by the authorities or who had learned of the surveillance through criminal proceedings, while legal persons were excluded from this remedy altogether. Furthermore, the newly introduced data protection remedies were untested, unavailable to legal entities, and did not provide a concrete avenue for challenging unlawful surveillance. See also Pietrzak and Bychawska-Siniarska and Others v Poland (ECtHR, Apps nos 72038/17 and 25237/18, 28 May 2024), para 142–46.
[215] A L and E J v France (ECtHR, Apps nos 44715/20 and 47930/21, 24 September 2024), para. 113. Given the importance of the case, it would have been far preferable for a full Chamber - if not even the Grand Chamber - to have clarified the matter in a full-fledged judgment.
[216] *Ibid.*, para. 114.
[217] *Ibid.*, para. 131-143.
[218] Bykov v Russia [GC] (ECtHR, App no 4378/02, 10 March 2009), para. 78.

3. **Necessary in a democratic society meaning** that there must be a pressing social need, the interference must be proportionate to the legitimate aim pursued, while a state enjoys a certain margin of appreciation. However, exceptions must be interpreted narrowly.[219]

The Court clarified some key concepts regarding interceptions early on in *Klass and Others*,[220] assessing German legislation providing for surveillance in 'exceptional circumstances.' The applicants, including judges, lawyers, and public prosecutors, were never actually subjected to surveillance, but argued that the system allowed for such measures without notification or judicial review.[221] The Court accepted the legitimacy of secret surveillance of mail, post, and telecommunications under exceptional conditions and recognised a degree of national discretion.[222]

However, it emphasised that there is no unlimited discretion and that adequate and effective guarantees must exist. An assessment always depends on **all the circumstances of the case** (e.g., nature, scope and duration of measures, grounds for ordering, competent authorities, remedy). The Court recognised the importance of judicial authorisation, stating that '*judicial control offering the best guarantees of independence, impartiality and a proper procedure*.'[223] However, it allowed that such control may be replaced by adequate parliamentary control.[224]

It is thus clear from Article 8(2) that interception and other secret surveillance measures may be used, *inter alia*, for purposes of national security, public safety, prevention of disorder or crime, as well as to protect the rights and freedoms of others. In that regard, justification will not usually be a problem in terms of the tri-partite test. Instead, possible infringements tend to concentrate either separately or cumulatively[225] on parts 1 and 3 of the above-mentioned test, namely legality and proportionality.

7.1.3.1 In accordance with the law

Often, national systems do not satisfy the first element – '*in accordance with the law*,' whereby the Court stops its analysis here, or sometimes makes a joint assessment of the 'accordance of law' and 'necessary in a democratic society' criteria. For example, in *Huvig*,[226] legislation did not explicitly authorise investigating judges to order telephone surveillance; rather, judges assumed this power based on their general investigative authority. French courts accepted such measures under certain conditions (e.g. disclosure of original recordings to the defence, respect for lawyer–client confidentiality). In this case, the recordings were not used as the basis for prosecution, but the Court considered that fact irrelevant (important only regarding potential damages). The Court held that the law did provide authorisation for surveillance, stating that the Court considered law in a substantive sense, not a formal one. It can also compromise of rules below, as well as

[219] The Court will determine whether unlawful surveillance occurred based on the totality of circumstances, and there need not be direct evidence of surveillance. See Iliya Stefanov v Bulgaria (ECtHR, App no 65755/01, 22 May 2008), para. 50.
[220] Klass and Others v Germany (ECtHR, App no 5029/71, 6 September 1978), regarding Germany's 1968 surveillance law.
[221] *Ibid.*, para. 34-38.
[222] *Ibid.,* para. 49.
[223] *Ibid.*, para. 55.
[224] *Ibid.*, para. 56.
[225] Pietrzak and Bychawska-Siniarska and Others v Poland (ECtHR, Apps nos 72038/17 and 25237/18, 28 May 2024).
[226] Huvig v France (ECtHR, App no 11105/84, 24 April 1990). See also Valenzuela Contreras v Spain (ECtHR, App no 27671/95, 30 July 1998), para. 60-61.

unwritten law.[227] The problem, according to the Court, did not lie in the accessibility of the law, but in the foreseeability of its consequences, and it found that the system lacked sufficient safeguards.[228]

In *Kopp*,[229] the Court raised the issue of foreseeability regarding the distinction between matters specifically connected with a lawyer's work under instructions from a party and those relating to other activity, and stated that '[a]bove all, in practice, it is, to say the least, astonishing that this task should be assigned to an official of the Post Office's legal department, who is a member of the executive, without supervision by an independent judge, especially in this sensitive area of the confidential relations between a lawyer and his clients, which directly concern the rights of the defence. In short, Swiss law, whether written or unwritten, does not indicate with sufficient clarity the scope and manner of exercise of the authorities' discretion in the matter.'[230]

In *Roman Zahkarov*[231] and *Ekimdzhiev*[232] the Court defined the **elements of the in accordance with law criteria** as: (i) the nature of the offences; (ii) persons covered, (iii) duration and limit of the secret surveillance measures, (iv) the procedure to be followed for examining, using and storing the data obtained; (v) the precautions to be taken when communicating the data to other parties; and (vi) the circumstances in which intercepted data may or must be erased or destroyed.[233] It further added: (vii) the arrangements for supervising the implementation of secret surveillance measures, (viii) any notification mechanisms, and (ix) the remedies provided for by national law.[234] In *Pietrzak*, the Court found a violation due to the lack of content in the authorisation, the absence of reasoning except in cases of rejection, an unclear emergency procedure, inadequate deletion procedures, insufficient protection of lawyer–client privilege, the limitation of court oversight to the authorisation phase only, and the lack of notification and effective remedies.[235]

Further, the Court distinguished between **authorisation of the measure** and **implementation of the measure**. Regarding the first, it pointed to the type of authority authorising, and offences covered, scope of affected persons, and possibility of accumulation of orders timewise. Regarding application, it highlighted the role of judicial oversight, a clear level of suspicion, the manner of screening of the obtained evidence, its integrity, confidentiality and deletion, and the importance of the lawyer-client privilege.[236]

7.1.3.2 Necessary in a democratic society

[227] *Ibid.*, para. 28.
[228] *Ibid.*, para. 34.
[229] Kopp v Switzerland (ECtHR, App no 23224/94, 25 March 1998).
[230] *Ibid.,* para. 75.
[231] ECtHR, *Roman Zakharov, supra*, para. 235-305, regarding overly broad and vague conditions for authorising surveillance, absence of meaningful judicial review, and lack of safeguards against abuse (e.g., judicial authorisation only formal, direct access by law enforcement, weak prosecutorial supervision, no notification mechanism, no effective remedy).
[232] ECtHR, *Ekimdzhiev, supra*, para. 291-359, regarding inaccessible internal rules on data handling, vague legal definitions, excessive duration, inadequate judicial scrutiny, gaps in rules governing storage, use, and destruction of data, lack of sufficiently independent and empowered oversight, ineffective notification procedures, inadequate remedies, not open to legal persons and limited to monetary damages.
[233] ECtHR, *Ekimdzhiev*, *supra*, para. 76.
[234] ECtHR, *Romah Zakharov*, *supra*, para. 238. The criteria were summarised in this way in ECtHR, Big Brother Watch and Others v United Kingdom [GC] (ECtHR, Apps nos 58170/13, 62322/14, 24960/15, 25 May 2021).
[235] ECtHR, *Pietrzak, supra*, para. 207-246.
[236] ECtHR*, Iordachi*, *supra*, para. 43-48.

There is a certain overlap between the first criterion and this one regarding secret surveillance measures (e.g., adequate safeguards against abuses).[237] The third criterion basically refers to the **principle of proportionality** regarding the **balance between different interests**,[238] whereby the Court gave a c**ertain margin of appreciation to the states** (means for achieving the legitimate aim) under European supervision.

Hereby, the Court mainly assesses the '**adequate and effective guarantees against abuse'** based on 'all the circumstances of the case,' taking into account the nature, scope, and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out, and supervise them, and the kind of remedy provided by national law. **Judicial authorisation can be a strong countermeasure as regards a possible violation**.[239] The **severity of the interference** must be duly taken into account when assessing the applicable safeguards.[240] The Court scrutinises three stages of such surveillance, namely the **ordering stage**, the **execution stage**, and the **stage after termination**. The main difference is the lack of individual knowledge of the affected person during the first two stages and the question of notification at the third stage.[241]

Further, the Court held that it must be read to require '**strict necessity'** in two senses, namely as **general necessity** and **individual necessity**. General necessity means that secret surveillance must be strictly necessary to safeguard democratic institutions, not just desirable or useful. This is grounded in the potential for such powers to be abused and to undermine democracy under the guise of protecting it. Individual necessity means that each surveillance measure must also be strictly necessary to obtain vital intelligence in a specific case. There must be an **individualised factual basis** for targeting a person, with safeguards ensuring that authorities justify the measure's necessity and proportionality.[242] The Court also highlighted the importance of **reasonable suspicion** regarding facts or information capable of satisfying an objective observer that the person concerned may have committed the offence in question. However, such facts need not be at the same level as those required to justify a charge or a conviction.[243]

7.1.3.3 Targeted interception v. bulk interception

[237] Dragojević v Croatia (ECtHR, App no 68955/11, 15 January 2015), para. 101.
[238] L B v Hungary [GC] (ECtHR, App no 36345/16, 9 March 2023), para, 116.
[239] ECtHR, *Klass and Others*, *supra,* para. 56.
[240] Breyer v Germany (ECtHR, App no 50001/12, 30 January 2020), regarding the storage of certain data of prepaid mobile card users (e.g., name, address, date of birth, date of contract). The Court confirmed the measure stating, inter alia, that review and supervision are important but not decisive in proportionality assessment, considering the limited data set (para. 103). Compare to ECtHR, *Škoberne v. Slovenia*, a. no. 19920, judgment of 15 February 2024, para. 141, regarding an inadequate system of safeguards for gathering traffic data (general and indiscriminate system of data retention).
[241] ECtHR, *Roman Zakharov, supra*, para. 232-234.
[242] ECtHR, *Szabó and Vissy v. Hungary*, a. no. 37138/14, judgment of 12 January 2016, para. 72-73. The Court found a violation due to the scope of surveillance, including 'ranges of persons', no prior judicial authorisation or equivalent safeguards by an independent body, not merely political oversight (e.g. from a minister); and lack of effective remedies.
[243] ECtHR, *Karabeyoglu v. Turkey*, a.no. 30083/10, judgment of 7 June 2016, para. 103. The Court did not find a violation, as the applicant's telephone was tapped on the basis of reasonable suspicion, and the implementation of the measure was in compliance with the relevant legislation. In particular, the authorisation for the surveillance was granted by a court for protecting national security/maintaining order; the statutes/regulations provided strict conditions and were followed to the letter; the processing of the data complied with legal requirements and, finally, that data was destroyed within the statutory time limits.

Regarding new technical capabilities of states, the Court has substantially addressed the issue of bulk/mass interceptions. In the beginning, it followed the same approach for all kinds of interceptions.[244] However, in *Big Brother Watch*,[245] it **distinguished between targeted interception and bulk interceptio**n regarding the use of the above-mentioned criteria, as it highlighted that some are not applicable to bulk data (e.g., offences and scope of persons), while others gain additional importance (e.g., amplified importance of supervision and review).

Thus, the Court focused on '**end-to-end' safeguards** and developed joint criteria for both the quality of law and 'necessity in a democratic society,' namely:

1. the grounds on which bulk interception may be authorised;
2. the circumstances in which an individual's communications may be intercepted;
3. the procedure to be followed for granting authorisation by an indeopendent body (but not necessarily a court);
4. the procedures to be followed for selecting, examining and using intercept material;
5. the precautions to be taken when communicating the material to other parties;
6. the limits on the duration of interception, the storage of intercept material, and the circumstances in which such material must be erased and destroyed;
7. the procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;
8. the procedures for independent ex post facto review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.[246]

This also applies to the extraterritorial use of bulk interception measures and implies the responsibility of the State using them.[247] The interference takes place where 'communications are intercepted, searched, examined and used and the resulting injury to the privacy rights of the sender and/or recipient will also take place there.'[248] A separate approach to bulk interception has been welcomed for providing safeguards for existing mass surveillance, as well as criticised for establishing mass surveillance as an acceptable norm, thus backtracking from a prior level of suspicion for a person regarding an offence and establishing the preventive state.[249]

The Court precluded **general and indiscriminate systems of access/metadata data retention** mandated to private providers. In the case of *Pietrzak,* it applied the test for secret surveillance (*Ekimdzhiev*) and found illegal a 12-month indiscriminate retention regime allowing direct access

[244] ECtHR, *Liberty and Others v. UK*, a. no. 58243/00, judgment of 1 July 2008, para. 62. See also ECtHR, *Weber and Saravia v. Germany*, a. no. 54934/00, decision of 29 June 2006, para. 95.
[245] ECtHR, *Big Brother Watch, supra,* para. 340-347.
[246] *Ibid.*, para. 236. The Court found a violation because the UK's bulk interception regime lacked independent authorisation, failed to include categories of selectors in the warrant application, and did not subject selectors to prior internal authorisation. See also Centrum för Rättvisa v Sweden [GC] (ECtHR, App no 35252/08, 25 May 2021), para. 275.
[247] Wieder and Guarnieri v United Kingdom (ECtHR, Apps nos 64371/16 and 64407/16, 12 September 2023).
[248] *Ibid.,* para. 94.
[249] Watt E, 'Much Ado About Mass Surveillance - The ECtHR Grand Chamber 'Opens the Gates of an Electronic Big Brother' in Europe in Big Brother Watch v UK' (2021) Strasbourg Observers, 30-73. It highlights how the Court backtracked from the first two criteria from *Weber and Saravia*, namely clear prior indication of nature of offences and categories of people; Loideain N, 'Not So Grand: The Big Brother Watch ECtHR Grand Chamber Judgment' (Information Law & Policy Centre Blog, 28 May 2021) https://infolawcentre.blogs.sas.ac.uk/2021/05/28/not-so-grand-the-big-brother-watch-ecthr-grand-chamber-judgment/ accessed 1 August 2025; Milanović M, 'The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för Rättvisa' EJIL: Talk! (26 May 2021) https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/ accessed 4 August 2025.

by law enforcement and intelligence services to such data, regardless of any connection to a crime. It also clarified that the v**ery existence of such a system constitutes an interference with Article 8 ECHR**, and that access to such data raises a separate question of violation.[250]

In *Podchasov,*[251] the Court found an even more serious intrusion, as retention of content data was required for a period of six months (e.g., Telegram), in addition to the one-year storage of other communication data, with direct access by state authorities and an obligation to provide a **decryption key** (end-to-end encryption). The Court reiterated its previous finding of inadequate safeguards, e.g., authorisation (*Roman Zakharov*). It refused introduction of decryption obligation, as it would, as foreseen, **weaken all users' encryption**, thus affecting everyone **indiscriminately**.[252]

7.1.4 Relationship between Articles 6 and 8 ECHR regarding fairness of proceedings and admissibility of evidence

A finding of violation of Article 8 ECHR **does not automatically lead to a violation of Article 6 ECHR** if such evidence is used.[253] This applies also to data gathered through an illegal data retention system, whereas the admissibility of such data is a separate matter to be assessed by national courts.[254] However, it might be different under possible higher standards of national constitutional law. Instead, the ECtHR uses a **weighting method** regarding influence on **fairness of the procedure**. In *Schenk*[255] the Court highlighted that '*[w]hile Article 6 of the Convention guarantees the right to a fair trial, it does not lay down any rules on the admissibility of evidence as such, which is therefore primarily a matter for regulation under national law. The Court therefore cannot exclude as a matter of principle and in the abstract that unlawfully obtained evidence of the present kind may be admissible. It has only to ascertain whether* [the] *trial as a whole was fair.*'[256]

Instead, the Court concentrates mainly of the **question if rights of the defence were disregarded**, namely **nature of violation**, if the person had the **opportunity of challenging** its authenticity and opposing its use, and if the evidence in question was the **only evidence** on which the conviction was based.[257] However, in *Khan*[258] the illegally obtained evidence in violation of

[250] ECtHR, *Pietrzak*, *supra*, para. 248-264. Seel also ECtHR, Mass surveillance, Factsheet, June 2024, https://www.echr.coe.int/documents/d/echr/fs_mass_surveillance_eng (accessed 1 August 2025); see n 9.
[251] Podchasov v Russia App no 33696/19 (ECtHR, 13 February 2024).
[252] *Ibid*., para. 76-79.
[253] See also Balázs Garamvölgyi et al., 'Admissibility of Evidence in Criminal Proceedings in the EU,' *Eucrim*, no. 3 (2020): 201-208; European Law Institute, *Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings*, 8 May 2023, accessed 1 August 2025, https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Proposal_for_a_Directive_on_Mutual_Admissibility_of_Evidence_and_Electronic_Evidence_in_Criminal_Proceedings_in_the_EU.pdf; Oleksii Kostenko and Vahid Akefi Ghaziani, 'Admissibility of Illegally Obtained E-Evidence: A Critical Study of EU Law and the Precedents of the European Court of Human Rights,' *European Journal of Privacy Law and Technologies* 2 (2024): 206–220; Lorena Bachmaier Winter and Farsam Salimi, eds., *Admissibility of Evidence in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair Trial Rights*, Hart Studies in European Criminal Law (Oxford: Hart Publishing, 2024).
[254] Škoberne v Slovenia (ECtHR, App no 19920/15, 15 February 2024), para. 146.
[255] Schenk v Switzerland (ECtHR, App no 10862/84, 12 July 1988).
[256] *Ibid*., para. 46.
[257] *Ibid*., para. 47-48.
[258] Khan v United Kingdom (ECtHR, App no 35394/97, 12 May 2000), regarding the use of a covert listening device (without a proper legal basis) to record the applicant confessing to drug importation.

Article 8 ECHR was the only evidence, and the Court did not find a violation of Article 6 ECHR. In that regard, it stated that '*the relevance of the existence of evidence other than the contested matter depends on the circumstances of the case. In the present circumstances, where the tape recording was acknowledged to be very strong evidence, and where there was no risk of it being unreliable, the need for supporting evidence is correspondingly weaker,*'[259] as the applicant could challenge authenticity and use.

Based on the mentioned test, in *P.G. and J.H.*[260] the Court found a violation due to covert audio surveillance of the apartment and police station cells, as there was a deficient statutory legal framework in place.[261] But the trial was considered fair, since the recording was not the only evidence, its admissibility could be challenged, and the voice sample did not contain any incriminating content.[262]

In *Bykov,*[263] the Court found that a covert operation (e.g., secret recording through a radio-transmitter) constituted a violation of Article 8 ECHR due to lack of clear, detailed, and accessible safeguards against abuse (e.g., no judicial control).[264] But it did not find a violation of Article 6 ECHR as the defendant was given full opportunity to challenge admissibility, the recording was not the sole/main evidence, and he voluntarily engaged in conversation. Further, the recording was used only as contextual evidence among a chain of evidence.[265]

7.2. CJEU case law

In Articles 7 and 8 Charter the rights to privacy and data protection are enshrined. Pursuant to Article 52(3) of the Charter, rights corresponding to those guaranteed by the ECHR must be interpreted in the same way, namely at least as protective as, the corresponding ECHR standards. However, the Charter applies only when EU law is being implemented (Article 51 of the Charter). Regarding surveillance/interception of communications, national security falls outside the scope of EU competence (Article 4(1) TEU).[266]

Nonetheless, the CJEU has delivered several judgments concerning surveillance/interception, including in contexts of telecommunication data retention touching upon national security, and international relations, by interpreting such issues through the lens of EU competences in data protection. This topic was also addressed in judgments concerning EU cross-border judicial cooperation in criminal matters, such as the use of the EIO (see Chapter 9 on EncroChat).

7.2.1 Telecommunication data retention

Telecommunications data retention refers to a system of mandatory retention of telecommunications traffic data for a defined period for all individuals, based on its potential future

[259] *Ibid.*, para. 37.
[260] P G and J H v United Kingdom (ECtHR, App no 44787/98, 25 September 2001).
[261] *Ibid.*, para. 56-63.
[262] *Ibid.*, para. 76-81. See also, Allan v United Kingdom (ECtHR, App no 48539/99, 5 November 2002), para. 46-48.
[263] Bykov v Russia [GC] (ECtHR, App no 4378/02, 10 March 2009).
[264] *Ibid.*, para. 69-83.
[265] *Ibid.,* para. 94-105.
[266] See also ECtHR, FRA; *supra*; Celeste E and Formici G, 'Constitutionalizing Mass Surveillance in the EU: Civil Society Demands, Judicial Activism, and Legislative Inertia' (2024) 25 German Law Journal, 427-446; Erbežnik A, 'Impact of Digital Evidence Gathering on the Criminal Justice System: A Broader Perspective' in Vanessa Franssen and Stanisław Tosza (eds), *The Cambridge Handbook of Digital Evidence in Criminal Investigations* (Cambridge University Press 2025) ch 1.

use in criminal prosecution. However, such retention is extremely sensitive in terms of **data protection** and the **right to privacy**, and it has triggered an extensive body of case-law from the CJEU, the ECtHR, and various national courts.

As mentioned before, most of the cases are closely connected to the right to data protection. The CJEU has developed a substantial body of case-law on data retention, particularly concerning metadata. We have witnessed an evolution from the Court's initial strict rejection of such practices to a more nuanced approach, based on distinctions between categories of data, grounds for retention, and targeted measures. The Court has also established certain common standards regarding authorising authorities and the admissibility of evidence.[267]

7.2.1.1 Prohibition of general and non-discriminate systems

In the EU, the now annulled **Directive 2006/24/EC** on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or public communications networks[268] introduced an obligation for Member States to impose mandatory retention of telecommunications traffic data for a period ranging from six months to two years.[269]

The **CJEU declared the Directive invalid** in ***Digital Rights Ireland***[270] due to a breach of proportionality under Articles 7 and 8 of the Charter. It noted that the Directive applies indiscriminately to everybody and is not limited to a particular period/geographical area and a group of persons.[271] It also highlighted the absence of procedural and substantive conditions regarding access by national authorities (e.g., specification of serious offences, lack of prior authorisation by court/independent administrative authority, tailored time limitation).[272] In *Tele2/Watson*,[273] the CJEU extended its prior finding to such national data retention systems, based on Directive 2002/58/EC,[274] and the Charter. Among other things, it stated that such

[267] Kosta E and Kamara I (eds), *Data Retention in Europe and Beyond: Law and Policy in the Aftermath of an Invalidated Directive* (Oxford University Press 2025); Celeste E, 'The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios' (2019) 15 European Constitutional Law Review, 134-157; Podkowik J, Rybski R and Zubik M, 'Judicial Dialogue on Data Retention Laws: A Breakthrough for European Constitutional Courts?' (2021) 19 International Journal of Constitutional Law 1597-1631.
[268] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC OJ L 105/54.
[269] *Ibid.*, Art. 6 .
[270] Case C-293/12 in C-594/12 Digital Rights Ireland and Kärntner Landesregierung et al (CJEU, 8 April 2014) ECLI:EU:C:2014:238. See also Lynskey O, 'The Data Retention Directive Is Incompatible with the Rights to Privacy and Data Protection and Is Invalid in Its Entirety: Digital Rights Ireland' (2014) 51(6) Common Market Law Review 1789.
[271] *Ibid.*, para. 58-59.
[272] *Ibid.*, para. 60-66.
[273] Case C-203/15 in C-698/15 Tele2 Sverige and Watson (CJEU, 21 December 2016) ECLI:EU:C:2016:970.
[274] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on privacy and electronic communications OJ L201/37.

systema allow precise conclusions on private lives creating a feeling of constant surveillance.[275] A number of national constitutional courts have adopted similar positions.[276]

7.2.1.2 Targeted systems

Already in *Tele2/Watson* the Court indicated the possibility of **targeted data retention** of traffic/location data for combating serious crime, provided the retention is **limited to what is strictly necessary** - in terms of categories of data, types of communications, persons involved, and duration, and provided clear and precise national legislation, including **minimum safeguards**.[277] Further, in *Ministerio Fiscal*,[278] the CJEU allowed access to **identification data of SIM card holders** activated via stolen mobile phones for criminal offences (e.g., name, address).[279]

In follow up cases *Privacy International*[280] and *La Quadrature du Net et al.*,[281] it permitted general retention of subscriber data and IP addresses, targeted retention of location and traffic data, and exceptions to the general prohibition of indiscriminate retention, in cases of national security, serious crime and serious threats to public security.[282] It proscribed also certain conditions, such as **effective review** by a court or independent administrative body, and time limits.[283] Measures in line with EU law are:

- General and indiscriminate retention of traffic/location data in situations where a Member State is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable;
- Targeted retention of traffic/location data, which is limited, based on objective and non-discriminatory factors, according to the categories of persons/geographical criterion, for safeguarding national security, combating serious crime and preventing serious threats to public security;
- General and indiscriminate retention of IP addresses assigned to the source of an Internet connection, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security;
- General and indiscriminate retention of data relating to the civil identity of users of electronic communications system, for the purposes of safeguarding national security, combating crime and safeguarding public security;

[275] *Ibid.*, para. 100. See also Cases C-793/19 and C-794/19 SpaceNet and Telekom Deutschland (CJEU, 20 September 2022) EU:C:2022:702, regarding annulment of the German general system despite being limited to several weeks only; Case C-350/21 Spetsializirana prokuratura (CJEU, 17 November 2022) EU:C:2022:896, regarding a Bulgarian six-month general system; Case C-339/20 VD and SR (CJEU, 20 September 2022) EU:C:2022:703, regarding a French one-year general system regarding market abuse offences.
[276] Zubik M et al, *European Constitutional Courts towards Data Retention Laws* (Springer 2021); Fennelly D, 'Data retention: the life, death and afterlife of a directive' (2019) 19 ERA Forum 673–92.
[277] Ibid., para. 108-109.
[278] Case C-207/16 Ministerio Fiscal (CJEU, 2 October 2018) ECLI:EU:C:2018:788.
[279] European Digital Rights (EDRi), 'CJEU Introduces New Criteria for Law Enforcement to Access Data' (24 October 2018) https://edri.org/our-work/cjeu-introduces-new-criteria-for-law-enforcement-to-access-to-data/ accessed 1 August 2025.
[280] CJEU, Case C-623/17, *Privacy International*, judgment of 6 October 2020, ECLI:EU:C:2020:790.
[281] Cases C-511/18, C-512/18 in C-520/18 La Quadrature du Net et al. (CJEU, 6 October 2020) ECLI:EU:C:2020:791.
[282] *Ibid.*, para. 87-104.
[283] *Ibid.*, para. 134-139.

- Expedited retention of traffic and location data, for the purposes of combating serious crime and safeguarding national security.[284]

7.2.1.3 Authorisation authorities

In *H.K.*,[285] the Court **denied prosecutors the authority to approve access to traffic/location data.** It clarified that an independent authority must have a status ensuring **objective and impartial action**, protected from **external influence**, **not be involved** in investigating the criminal offence in question, and be **neutral**. In that regard, the Court stated:

'54. It follows from the foregoing considerations that the requirement of independence that has to be satisfied by the authority entrusted with carrying out the prior review […] means that that authority must be a third party in relation to the authority which requests access to the data, in order that the former is able to carry out the review objectively and impartially and free from any external influence. In particular, in the criminal field […] the requirement of independence entails that the authority entrusted with the prior review, first, must not be involved in the conduct of the criminal investigation in question and, second, has a neutral stance vis-à-vis the parties to the criminal proceedings.'[286]

7.2.1.4. Admissibility of evidence

However, the CJEU clarified certain rules on the **(in)admissibility of evidence on data retained**, although acknowledging at the same time Member States' autonomy in this regard. It highlighted the **principle of adversarial proceedings**, asserting that 'the principle of effectiveness requires a national criminal court to exclude information and evidence obtained through general and indiscriminate retention of traffic and location data that is incompatible with Union law, where the accused cannot effectively comment on such evidence, which derives from a technical field beyond the court's expertise and may significantly affect the findings of fact.'[287]

7.2.2 EU-US data transfers

The second set of judgments regarding surveillance/interceptions refers to **EU personal data transfers to the United States**, whereby the EU-US frameworks have already been annulled twice. The main argument of the CJEU were unchecked **U.S. interception/surveillance prerogatives** regarding such data. In *Schrems I,*[288] the CJEU annulled EU-US *Safe Harbour*[289] due to mostly on unchecked U.S. national security and law enforcement access, as well as the lack of effective legal remedies. In *Schrems II*,[290] the CJEU annulled the subsequent EU-U.S. **Privacy Shield,**[291] focusing again on U.S. surveillance practices and disproportionate access to

[284] *Ibid.*
[285] Case C-746/18 H.K. (Prokuratuur) (CJEU, 23 March 2021) ECLI:EU:C:2021:152.
[286] *Ibid.,* para. 54. See also Case C-140/20 Garda Síochána (CJEU, 5 April 2022), para. 111-114, denying police authorities as authorisation authorities.
[287] CJEU, *La Quadrature du Net et al.*, *supra*, para. 221-228.
[288] Schrems (Maximillian) v Data Protection Commissioner (C-362/14) EU:C:2015:650. In its preliminary question the Irish High Court specifically referred to both, surveillance and interception (para. 30-33).
[289] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC on the adequacy of the protection provided by the Safe Harbour privacy principles OJ L215/7.
[290] Data Protection Commissioner v Facebook (Schrems II) (C-311/18) EU:C:2020:559.
[291] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC on the adequacy of the protection provided by the EU-US Privacy Shield OJ L207/1.

EU personal data. It took into account FISA Section 702 and Executive Order 12333 and the lack of effective legal remedies before U.S. courts, e.g. the Ombudsperson mechanism lacking independence. At the moment the existing EU-U.S. **Data Privacy Framework**[292] is in place, although in expectation of a possible *Schrems III* judgment.

7.3. National case law

7.3.1 Slovenia

Slovenian case law, both from the Constitutional Court and the Supreme Court, has examined in detail the issue of interference with the privacy of communications through telecommunications surveillance.

7.3.1.1 Use of Telecommunications Interception in Jurisprudence

7.3.1.1.1 Constitutional Framework and covered investigative measures

Early in the existence of independent Slovenia, the Constitutional Court, in its **Decision U-I-25/95 of 27 November 1997**, annulled the provisions of Articles 150 to 156 of the CPA, because it considered that 'eavesdropping [...] with technical devices constitutes an extreme interference with the constitutional right to privacy.' The Constitutional Court stated that 'eavesdropping [...] with technical devices is a serious interference with the constitutional right to privacy and must be based on very specific rules with clear and detailed rules.' It criticized the existing regulation, according to which the conditions for use were not sufficiently specific and in accordance with the requirement of proportionality in terms of necessity for the conduct or progress of criminal proceedings (second paragraph of Article 37 of the Constitution of the Republic of Slovenia). This decision referred not only to wiretapping but also to other measures from the set of so-called covert investigative measures. As a result, the aforementioned articles were amended relatively frequently and supplemented.

In its 1997 landmark decision, the Constitutional Court also established a constitutional framework for wiretapping, stating that wiretapping is not contrary to Articles 35 and 37 of the Constitution under the following conditions: (a) the interference shall be specifically defined and determined by law; (b) the interference shall be authorized by a court decision; (c) the duration of the interference is strictly limited; and (d) the interference is necessary for the initiation or conduct of criminal proceedings, whereby the principle of proportionality is taken into account when assessing necessity of the measure.

Of particular importance was also the Court's view in **Decision U-I-18/93 of 11 April 1996** that a higher degree of probability than mere suspicion that a criminal offense had been committed was required for wiretapping. It stated that there must be a higher degree of suspicion and that, in terms of the quality and quantity of the information gathered and its verifiability, it must largely approximate the grounds for suspicion. The latter means a high degree of articulated concrete and specific probability that a specific person has committed a criminal offense. This new standard of proof – reasonable grounds for suspicion – was then introduced into criminal proceedings by

[292] Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 on the adequate level of protection of personal data under the EU-US Data Privacy Framework OJ L231/118.

the CPA-A amendment and still constitutes the minimum basis for virtually all interventions that fall within the scope of covert investigative measures (see also Decision U-I-144/19, explained below).

As pointed out in Section 6.1.1, in its **Decision Up 412/03 of 8 December 2005**, the Constitutional Court ruled that the police must carry out wiretapping measures for the purposes of criminal proceedings and cannot transfer this power to the intelligence service (SOVA). In another decision (**U-I-8/04 of 22 June 2006**), the Constitutional Court stated that by regulating wiretapping in the CPA, the legislature does not interfere with the procedural rights under Article 29 of the Constitution of the Republic of Slovenia (in particular the privilege against self-incrimination) and that the determination of whether there has been a violation of the procedural rights of the defendant is linked to an assessment of whether the conditions and criteria under which the measure was ordered in each individual case were met under the above-mentioned conditions.

7.3.1.1.2. Judicial Authorisation and Procedural requirements

In **Decision Up 2094/06 of 20 March 2008**, the Constitutional Court stated that, when using covert investigative measures, consistent compliance with the legal provisions on the procedure for ordering covert investigative measures is not merely a formalistic requirement. This is a mechanism that the court must apply in such a way as to prevent the possibility of abuse in the gathering of evidence. Therefore, the fact that the police initiative and the public prosecutor's proposal must be substantiated does not relieve the investigating judge of the obligation to justify the existence of the legal conditions for the introduction of the measure. Following this decision, the investigating judge must state in the orders the facts and circumstances giving rise to reasonable grounds for suspecting that criminal offences have been committed and reasonable grounds for suspecting that certain means of communication are being used in the commission of criminal offences, and justify the absolute necessity of using the measure in relation to gathering evidence by other means (the urgency of gathering evidence in this way).

With regard to the subject matter of the INCEPT project, the **Decision Up 995/15 of 12 July 2018** is of particular importance. The Constitutional Court ruled that the rights of the accused had been violated because the court had not obtained court orders from abroad with which the accused had been placed under telephone surveillance in criminal proceedings. The Constitutional Court was of the opinion that it is necessary to obtain such orders from foreign judicial authorities in order to assess the admissibility or inadmissibility of evidence obtained on the basis of foreign orders.

In its **Second partial decision U-I-144/19 of 1 December 2022**, which we referred to in Section 6.1.1.1, the Constitutional Court abrogated point 1 of the first paragraph of Article 150a and several paragraphs of Article 150 of the CPA in connection with the provision of point 1 of the first paragraph of Article 150.a of the CPA, which regulates the surveillance of communications. Dealing with the use of the IMSI catcher, the Court stated that, due to the nature and scope of the interference, the investigating judge must have the possibility to carry out thorough subsequent judicial review on the basis of the material collected. They must be able to see when, how many times, how, and for what reason the IMSI catcher was used and to verify the connection between the order issued and the use of the IMSI catcher in the specific case.

In **Decision Up-106/05-27 of 2 October 2008**, the Constitutional Court stated, among other things, that it is erroneous to consider that the police may obtain data that fall within the scope of

constitutionally protected privacy of communications without a court order in pre-trial proceedings. In the case in question, a SIM card was seized, from which the police obtained information about stored electronic data related to the suspect's telecommunications (e.g., telephone numbers called, and text messages sent). The Constitutional Court ruled that this constituted an interference with freedom of communication and that prior court authorization was therefore required.

The Constitutional Court's **Third partial decision U-I-144/19 of 6 July 2023**, referred to in Section 6.1.1.1.1 of this report, found several provisions of the CPA relating to communication privacy unconstitutional and sparked considerable debate among the legal community. In this decision, the Constitutional Court first ruled that the acquisition of data relating to the communications of suspects, defendants, or injured parties constitutes an interference with the privacy of communications and that the legal regulation of this interference does not pass the test of proportionality in the strict sense, because the severity of the consequences of the measure, given the low standard of proof required for grounds for suspicion, the absence of a time limit for the contested measure, and the existing overly broad catalogue of criminal offences outweigh the benefits of the measure. The legislature responded to the court's decision by setting a higher standard of proof or stricter conditions for obtaining such data (see Section 6.1.1.1 of this report for more detailed presentation of the legislative developments following the Constitutional Court's third partial decision).

This decision was preceded by the **Decision U-I-65/13 of 26 September 2013**, which repealed several provisions of the Electronic Communications Act (ZEKom-1) that allowed for the mandatory and non-selective storage of certain traffic data of all communications in fixed-line telephony, mobile telephony, internet access, internet e-mail, and electronic communications via internet. In this case, the Constitutional Court based its decision on the finding that the storage of such data constitutes a significant interference with the right to the protection of personal data and that the contested measure is not strictly necessary.

7.3.1.1.3 Catalogue of Qualifying Offences and Proportionality

As pointed out in Section 6,1, criminal offenses for which wiretapping may be ordered are defined in the second paragraph of Article 150 of the CPA. Interestingly, there is a significantly wider list of criminal offences for certain investigative measures that do not directly interfere with the privacy of communications (a list of these criminal offences is defined in the fourth paragraph of Article 149.a of the CPA). Both the decision (para. 60) and the separate opinion of Constitutional Court Judge Katja Šugman Stubbs in case **U-I-144/19-52 of 2 August 2023**, show that the court is of the opinion that the catalogue or list of criminal offences for which the measures under Article 149.a of the CPA can be ordered is too broad and that the measures need to be regulated in such a way that they are proportionate to the detection, prosecution, and proof of serious criminal offences within the meaning of established constitutional court case law and the practice of the CJEU and the ECtHR. Regarding criminal offences from the second paragraph of Article 159, it follows from the above Constitutional Court's decision, by *a contrario* reasoning, that the definition of these criminal offences must be strictly observed.

The Supreme Court of the Republic of Slovenia has, however, ruled in several decisions that the results of communications surveillance may also be used as the basis for a criminal offense not included in the list (the non-qualified form of criminal offence) if, at the time the order was issued,

there were reasonable grounds to suspect that a qualified form of criminal offense had been committed, e.g., an act for which the measure could be ordered (**Judgments I Ips 292/2004** and **Ips 264/2005**).

7.3.1.1.4 Safeguards and Procedural Protections

The practice of the Constitutional Court and regular courts shows that the exclusion of evidence is one of the key elements in ensuring the procedural rights of the accused. Given the nature of covert investigative measures, this instrument is in fact the only means of defence available to challenge the constitutionality and legality of such interference with the procedural rights of the accused.

The Constitutional Court has stated in its **Decision Up-62/98 of 1 July 1999** that violations of constitutional rights committed in pre-trial proceedings by state authorities are subject to review by the Constitutional Court when deciding on a constitutional complaint against a conviction to the extent that there is a causal link between the conduct alleged to be unconstitutional by the complainant and the conviction. This means that violations of constitutional rights in a constitutional complaint against a conviction can only be invoked if the evidence on which the judgment is based was obtained through such a violation.

The Supreme Court has confirmed its position on the exclusion of evidence as part of the procedural guarantees of the accused in several decisions. For example, in its **Judgment I Ips 44415/2010 of 26 November 2021**, the Supreme Court clearly stated that in Slovenian criminal proceedings, it is prohibited to base a court decision on unconstitutional or unlawfully obtained evidence or its 'fruits' (second paragraph of Article 18 of the CPA), as this is a fundamental element of a fair trial. In situations of unconstitutional or unlawful conduct by state authorities, the utilitarian (instrumental) doctrine of exclusion of evidence has never been accepted. Exclusion is an institution of the autonomous (as opposed to ancillary) position of criminal proceedings in relation to substantive criminal law or the principle of seeking 'material' truth. If the prosecution fails to prove that the police acted in a constitutionally compliant and lawful manner in the pre-trial proceedings, the burden of proof cannot be shifted to the defendant (or the defence), as this would (also) violate the presumption of innocence under Article 27 of the Constitution. It follows from the reasoning of this decision that the decision on the exclusion of evidence is inextricably linked to the exercise of the right to judicial protection due to violations of human rights under the fourth paragraph of Article 15 of the Constitution.

The Supreme Court **Judgment I *Ips* 4259/2018 of 5 June 2020** states that the essence of a fair trial in deciding on exclusion requests is that the defence has an effective opportunity to challenge the use of evidence in a way that ensures equality of arms. Deciding on a request for the exclusion of evidence is – in the case of alleged violations of constitutionally protected rights – a form of judicial protection of human rights and a form of remedying the consequences of their violations. If the collection and selection of information relevant to the defence of the accused is in the hands of the police, the public prosecutor, or the court, the effective exercise of the right to adequate opportunities to prepare a defence depends on their conduct (collection and selection of information). The responsibility of the criminal justice authorities is all the greater when they act in secret from the public and other participants in the criminal proceedings.

It is clear from certain decisions (e.g., **Judgment VSRS I Ips 322/2008**, **Decision VSK Kp 229/2006**) that evidence gathered through covert investigative measures may be used against another person if, in executing an order within the scope for which it was issued, the law enforcement authorities unintentionally or accidentally come across evidence that is incriminating.

Overall, the examples of judgments cited above, which are based on established case law, show that the exclusion of illegal evidence is a fundamental instrument of subsequent judicial review of the legitimacy of interference with the privacy of communications under the provisions of the CPA. The Supreme Court first clearly defined the burden of proof of the prosecution, which is obliged to demonstrate that the police acted in accordance with the Constitution and the law, and secondly, that the defence is guaranteed an effective opportunity to object to the use of evidence.

Challenges for EIO and Cross-Border Cooperation:

- **Interpretation of the EIO Directive**: When applying the Directive with regard to both the incoming and outgoing EIOs, it may be unclear whether measures related to the real-time interception of telecommunications (such as transmission of stored traffic data related to a conversation for example) fall under the specific provisions on telecommunications interception or whether they are subject to the general regime of the EIO Directive.
- **Differences between legal frameworks**: Types of measures, competent authorities, lists or categories of offences for which interception is permitted, thresholds and prerequisites for judicial authorisation, time limits and duration rules in Slovenia may differ from those in other Member States, potentially causing delays or refusal of EIO requests for telecommunications interception.
- **Invoking grounds for non-recognition or non-execution**: The fact that Slovenian courts apply strict evidence exclusion rules may stimulate refusals of EIO requests for telecommunications interception.
- **Executing Trojan horse surveillance:** Trojan horse surveillance is permitted and used in most of the Member States but not in Slovenia. As a result, incoming EIOs for interception by using such technology cannot be recognized and executed. This means that in Slovenia, the possibilities for effective interception are limited, particularly when dealing with encrypted telecommunications.

7.3.1.2 Use of Evidence Obtained Abroad

7.3.1.2.1 Mutual Legal Assistance Framework

Slovenian courts regularly examine the admissibility of evidence obtained abroad through mutual legal assistance instruments, as described in the overview of legislation in Section 6.1. However, case law addressing issues related to both the outgoing and incoming EIOs cannot yet be identified in existing databases. The only recorded case which dealt with a EIO, concerned the question of whether the investigating judge had interfered with the execution of a EIO by subsequently sending an electronic message to the executing state in which she stated that certain information should not be transmitted. The Higher Court in Ljubljana did not consider the message to be an interference with the legeal provisions on the EIO and therefore did not find any violation of criminal procedure (**Judgment of the Higher Court in Ljubljana VI Kp 34126/2021 of 23 November 2023**).

7.3.4.2.2 Admissibility Standards for Foreign Evidence

The Constitutional Court ruled on the admissibility of evidence from abroad in **Decision Up-127/16 of 20 January 2022**. It stated that the inability to use evidence from abroad solely because the manner in which it was obtained (which could otherwise be in accordance with a foreign constitution) did not comply with the fundamental procedural guarantees of the Slovenian Constitution would result in the ineffectiveness of criminal proceedings before Slovenian courts. This would violate the positive obligation of the state to ensure the safety of persons within its territory. In this case, according to the Constitutional Court, the right to equality of arms was guaranteed to the accused by the fact that the court verified: (a) whether the constitutional procedural guarantees of the Italian Constitution protect against arbitrary police interference in a manner comparable to that of the Slovenian Constitution; (b) whether these guarantees were respected in the acquisition of evidence; (c) whether there was a legal basis for the interference; and (d) whether the interference was authorized by a competent judicial authority. The Constitutional Court has drawn a distinction between the collection of evidence abroad and its use within the Slovenian legal system. It held that, in principle, the acquisition of evidence by foreign law enforcement authorities outside the territorial jurisdiction of the Slovenian Constitution, and without the involvement of Slovenian authorities, does not constitute a violation of the Slovenian Constitution, even if the evidence was obtained under rules different from those in Slovenia. However, the Court emphasized that the fundamental procedural rights of the accused, as guaranteed by the Slovenian Constitution, must be respected when such evidence is used in criminal proceedings in Slovenia.

In a later **Decision Up-899/16-18, Up 900/16-25, Up901/16-25 of 5 May 2022**, the Constitutional Court confirmed the validity of foreign evidence obtained through covert investigative measures carried out by foreign authorities (the US) at their own initiative, because they were carried out in accordance with foreign law and at the same time were not obtained in violation of constitutionally guaranteed human rights and rights under the ECHR.

Also important is Constitutional Court **Decision Up 995/15 of 12 July 2018,** in which the Constitutional Court ruled that the rights of the accused had been violated because the court did not obtain foreign orders ordering the monitoring of telephone conversations against the defendant in criminal proceedings. The Constitutional Court was of the opinion that it is necessary to obtain such orders from foreign judicial authorities in order to assess the admissibility or inadmissibility of evidence obtained on the basis of foreign orders.

The Supreme Court of the Republic of Slovenia and the courts of appeal in the Republic of Slovenia follow these principles, and several decisions based on them have been adopted. In one of its most notable decisions (in the so-called 'Balkan Warrior' case), the Supreme Court assessed, among other things, the defence's arguments regarding the legality of evidence obtained abroad (**Judgment I Ips 44415/2010 of 26 November 2021**).The Supreme Court stated that it follows from the established and uniform practice of the Constitutional Court and the Supreme Court that evidence obtained independently in a foreign sovereign state against a person prosecuted there is admissible, even if the procedural or investigative acts were not carried out in accordance with the provisions of the CPA, provided that no guarantees under international law (conventions) or constitutional law were violated in the acquisition of the evidence. The decision is important because it deals with evidence obtained in a member state of the Council of Europe and Uruguay, e.g., countries that are not parties to the Convention on Mutual Legal Assistance. In the case in question, no such violations were found in either the Serbian or Uruguayan evidence. With regard to the evidence from Serbia, the Supreme Court

agreed with the reasoning of the lower courts, which had examined the duration of the measure in question against the suspect in the light of the standards established in the practice of the ECtHR (the Supreme Court of the Republic of Slovenia referred to the cases of *Malone v. the United Kingdom*, I*ordachi and Others v. Moldova,* and *Uzun v. Germany*). The Supreme Court considered it appropriate that the lower courts had proceeded from the assumption that, in assessing the proportionality of the duration of the measure, it was necessary to evaluate the seriousness of the criminal offense or the degree of threat to legally protected interests, which, given the fact that the investigation concerned an international criminal organization involved in illegal trafficking with drugs, was a legitimate reason for the interference with the suspect's right to privacy of communication. In the opinion of the Supreme Court, the procedural law of Serbia governing the maximum duration of interception was clear and specific, even at the critical time, and therefore predictable. According to the Court, it could not be argued that the conduct of the Serbian (judicial) authorities was arbitrary or capricious due to the sequence of procedural events. The same position was taken with regard to the evidence obtained during the house search of the yacht in Uruguay, which was attended by their investigating judge and not by solemn witnesses or the owner of the yacht, as would have been required under the provisions of the Slovenian CPA. According to the Supreme Court, the assessment of the fact that neither A. L. nor two solemn witnesses were present during the house search must be based on a comparison between the constitutionally guaranteed human rights in both countries, e.g., in the Republic of Slovenia and in the other country where the alleged violations were committed. In doing so, it is necessary to limit the assessment to whether the human rights that are alleged to have been violated are protected on both sides and whether their protection is guaranteed by (legal) judicial protection (fourth paragraph of Article 15 of the Constitution).

Slovenian courts have produced extensive case law on the admissibility of evidence obtained abroad; however, they have not yet explicitly addressed the admissibility of evidence obtained through the EIO mechanism. The case law described above illustrate the position of the Constitutional Court and the Supreme Court that it is necessary to assess relatively precisely the provisions of the positive law of a foreign country when deciding on the admissibility of evidence obtained abroad. The fundamental rights of the accused under the Slovenian Constitution must be respected when using foreign evidence in criminal proceedings in the Republic of Slovenia. There is no reason why this should not apply also to cases of cross-border obtaining of evidence from other Member States through the EIO mechanism.

Challenges for EIO and Cross-Border Cooperation:

- **General admissibility standards:** Although Slovenian case law does not explicitly address the admissibility of evidence obtained through EIOs, it is reasonable to assume that courts would still need to examine the relevant foreign legislation to determine whether the evidence meets the existing admissibility criteria.
- **Fundamental Rights Protection**: Differences in procedural rules and approaches to evidence gathering across Member States may not, by themselves, lead to admissibility issues in Slovenian criminal proceedings. However, such differences can raise concerns regarding the protection of fundamental rights, which may result in challenges to admissibility and, potentially, the exclusion of foreign evidence, including that obtained by telecommunications interception.

- **Evidence Exclusion Rules**: Slovenian courts apply strict evidence exclusion rules. The fundamental procedural guarantees (e.g., fundamental rights) of the accused under the Slovenian Constitution must be respected when using evidence obtained through the EIO in criminal proceedings in the Republic of Slovenia.

7.3.1.3 Synthesis: Implications for Cross-Border Judicial Cooperation

The Constitutional Court and the Supreme Court have developed extensive case law on the legal framework and use of covert investigative measures, including telecommunications interception, as well as on the admissibility of evidence obtained abroad. However, with the exception of a single case, Slovenian case law has not yet specifically addressed issues related to the cross-border collection of evidence through EIOs, including those involving telecommunications interception. Similarly, no publicly available Slovenian cases explicitly examine the criteria for the admissibility of evidence obtained abroad via EIOs.

Nevertheless, Slovenian courts and prosecution offices regularly collect evidence across borders, including through the EIO mechanism (over the past five years, courts alone have issued an average of more than 650 EIOs annually). The analysis of existing Slovenian case law on communications interception and evidence admissibility highlights several challenges for cross-border cooperation in general, and for the EIO mechanism in particular. These challenges include, among other, differences in legal frameworks, grounds for refusal, admissibility standards, rules on evidence exclusion, and human rights considerations.

7.3.2 Bulgaria

Bulgarian jurisprudence on special intelligence means (SIM) reveals a mature constitutional framework that nonetheless faces frictions when evidence must be used cross-border under the EIO. Section 7.3.2.1 maps national case-law on the deployment of telecommunication interception; Section 7.3.2.2 analyses judicial treatment of evidence originating abroad. Each major section concludes with a concise catalogue of challenges for EIO-based cooperation.

7.3.2.1 Use of Telecommunications Interception in Jurisprudence

7.3.2.1.1 Constitutional Framework and Special Intelligence Means

The Bulgarian approach to telecommunications interception is governed by a comprehensive legal framework anchored in the **Special Intelligence Means Act (SIMA)** of 1997, which establishes the fundamental principles for the use of special intelligence means in criminal proceedings. The **Decision 1/ 10.02.1998 on constitutional case № 17/1997 of the Constitutional Court** and the **Decision 10/ 28.09.2010 on constitutional case № 10/ 2010 of the Constitutional Court** have shaped the constitutional boundaries for surveillance activities, emphasising the need for judicial oversight and proportionality in the application of special intelligence means.

The **Decision 10/ 15.11.2011 on constitutional case № 6/2011 of the Constitutional Court** further refined these principles, establishing that any interference with telecommunications must meet strict constitutional requirements regarding the protection of privacy and correspondence. These constitutional decisions provide the foundational framework within which

all telecommunications interception must operate, ensuring that surveillance measures remain within the bounds of constitutional protection of fundamental rights.

7.3.2.1.2 Judicial Authorisation and Procedural Requirements

Bulgarian jurisprudence demonstrates a strong emphasis on judicial control over telecommunications interception. The **Judgment 516/ 16.12.2009 on criminal case № 539/ 2009** established important precedents regarding the procedural requirements for obtaining judicial authorisation for special intelligence means. Similarly, the **Judgment 44/ 10.04.2012 on criminal case № 3013/ 2011 of the Supreme Court of Cassation** confirmed that proper judicial authorisation is essential for the admissibility of evidence obtained through telecommunications interception.

The **Judgment № 83/ 19.06.2012 on criminal case № 3135/ 2011 of the Supreme Court of Cassation** and the **Judgment 273/ 08.08.2012 on criminal case № 796/2012 of the Supreme Court of Cassation** further elaborated on the procedural safeguards that must be observed when conducting telecommunications surveillance, establishing clear parameters for the legitimate use of such measures in criminal investigations.

7.3.2.1.3 Evidence Standards and Admissibility

The admissibility of telecommunications evidence in Bulgarian criminal proceedings is governed by strict standards established through case law. The **Interpretative decision 4/ 03.12.2014 on case № 4/ 2014 of the criminal division of the Supreme Court of Cassation** provided crucial guidance on how courts should evaluate evidence obtained through special intelligence means, establishing uniform standards for the assessment of such evidence.

The **Judgment 10/ 07.10.2015 on criminal case № 1646/ 2014 of the Supreme Court of Cassation** and the **Judgment 26/ 07.06.2016 on criminal case № 1626/2015 of the Supreme Court of Cassation** demonstrated the courts' commitment to ensuring that telecommunications evidence meets rigorous standards of reliability and procedural compliance before being admitted in criminal proceedings.

7.3.2.1.4 Professional Privilege and Protected Communications

A significant aspect of Bulgarian case law concerns the protection of privileged communications, particularly those between lawyers and their clients. Article 33 of the Law on the Bar Association establishes absolute protection for lawyer-client communications, stating that ‘conversations between a lawyer and his client may not be intercepted or recorded. Any recordings made may not be used as evidence and shall be subject to immediate destruction.’

The **Judgment 39 from 19.04.2012 on civil law case № 280/2010 of Regional court – Levski & Decision 1435 from 15.12.2012 on civil law case № 815/2012 of the Supreme Court of Cassation** and the **Judgment 378/ 29.06.2010 on criminal case № 188/ 2010 of the Supreme Court of Cassation** established clear precedents for the inadmissibility of evidence obtained

through the interception of lawyer-client communications, reinforcing the absolute nature of this protection.

Challenges for EIO and Cross-Border Cooperation:

- **Constitutional Standards Divergence**: Bulgaria's strict constitutional requirements for surveillance may exceed standards in other Member States, potentially causing refusal of EIOs that fail to meet Bulgarian constitutional thresholds
- **Professional Privilege Complications**: The absolute protection of lawyer-client communications in Bulgarian law may conflict with different privilege standards in other jurisdictions, complicating cross-border evidence sharing
- **Judicial Authorisation Requirements**: Bulgaria's emphasis on prior judicial authorisation may clash with administrative authorisation systems in other Member States
- **Evidence Exclusion Standards**: Strict Bulgarian standards for evidence admissibility may result in the rejection of telecommunications evidence obtained abroad under different procedural regimes

7.3.2.2 Use of Evidence Obtained Abroad

7.3.2.2.1 European Investigation Orders and Procedural Compliance

Bulgarian courts have addressed the use of evidence obtained through EIOs in several significant cases. The **Judgment 113/ 13.10.2020 on criminal case № 224/ 2019 of the Supreme Court of Cassation** and the **Judgment 208/ 07.05.2025 on criminal case № 78/ 2025 of the Supreme Court of Cassation** demonstrate the Bulgarian judiciary's approach to evidence obtained through international cooperation mechanisms.

These cases establish that evidence obtained through EIOs must comply with both Bulgarian procedural requirements and the standards outlined in the EIO Directive, ensuring that fundamental rights protections are maintained in cross-border cooperation scenarios.

7.3.2.2.2 European Court of Human Rights Jurisprudence

Bulgarian surveillance practices have been subject to extensive scrutiny by the European Court of Human Rights. The *Case of the Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria***,** Application No. 62540/00 established that Bulgarian surveillance laws at the time lacked adequate safeguards against abuse, leading to significant legal reforms.

The *Case of Iliya Stefanov v Bulgaria***,** Application No. 65755.01, *Case of Goranova-Karaeneva v Bulgaria*, Application No. 12739/05, *Case of Hadzhiev v Bulgaria*, Application No. 22373/04, *Case of Savovi v Bulgaria*, Application No. 7222/05, and C*ase of Vasil Vasilev v Bulgaria*, Application No. 7610/15 have collectively shaped Bulgarian surveillance law, establishing minimum standards that must be met for evidence to be admissible in cross-border proceedings.

The *Case of Ekimdzhiev and Others v Bulgaria*, Appl. No. 70078/12 found continuing violations of Article 8 of the ECHR, concluding that Bulgarian surveillance laws, even after reforms, still lacked sufficient safeguards against arbitrariness and abuse.

7.3.2.2.3 Court of Justice of the European Union Cases

Bulgarian courts have been active in seeking preliminary rulings from the CJEU on EIO-related matters. The **Case C-324/17, Request for preliminary ruling from the Specialised Criminal Court in the criminal proceedings against Ivan Gavanozov (Gavanozov I)** addressed fundamental questions about the EIO framework and legal remedies.

The **Case C-724/19, Request for preliminary ruling from the Specialised Criminal Court in the criminal proceedings against HP**, **Case C-852/19, Request for preliminary ruling from the Specialised Criminal Court in the criminal proceedings against Ivan Gavanozov (Gavanozov II)**, **Case C-349/21, Request for preliminary ruling from the Specialised Criminal Court in the proceedings against H.YA., I.P., D.D., Z.I., S.S. (H.YA. and Others I)**, and **Case C-229/23, Request for preliminary ruling by the Sofia City Court in the criminal proceedings against H.YA., I.P., D.D., Z.I., S.S. (H.YA. and Others II)** demonstrate the ongoing challenges in implementing the EIO framework in Bulgaria.

These cases reveal systematic issues with Bulgarian legislation that lacks adequate legal remedies against investigative measures, creating obstacles for effective cross-border cooperation.

7.3.2.2.4 Administrative Court Oversight

The **Judgment 8687/ 27.06.2018 on administrative case № 10518/ 2017 of the Supreme Administrative Court** addressed administrative aspects of surveillance oversight, establishing principles for the review of decisions related to special intelligence means and their impact on cross-border cooperation.

Challenges for EIO and Cross-Border Cooperation:

- **Structural Legal Deficiencies**: Bulgarian law's lack of adequate legal remedies against investigative measures, as highlighted in CJEU cases, creates fundamental obstacles to EIO implementation
- **ECtHR Standards Compliance**: Ongoing violations of Article 8 ECHR in Bulgarian surveillance practices may undermine mutual trust and recognition of evidence in cross-border cases
- **Remedies Gap**: The absence of effective legal remedies in Bulgarian law may prevent the country from issuing or receiving EIOs until legislative reforms address these deficiencies
- **Fundamental Rights Protection**: Bulgarian surveillance practices that fail to meet ECtHR standards may result in the rejection of evidence by courts in other Member States applying stricter human rights protections

7.3.2.3 Synthesis: Implications for Cross-Border Judicial Cooperation

The Bulgarian case law analysis reveals several critical challenges that impede effective cross-border judicial cooperation in telecommunications interception:

- **Constitutional and Legal Framework Gaps**: The ECtHR's findings in Ekimdzhiev and Others v Bulgaria highlight ongoing deficiencies in Bulgarian surveillance law that create obstacles to mutual trust in cross-border cooperation.

- **Procedural Inconsistencies**: The CJEU's rulings in the Gavanozov cases demonstrate that Bulgaria's legal framework lacks essential procedural safeguards, potentially precluding effective participation in EIO procedures.
- **Professional Privilege Conflicts**: The absolute protection of lawyer-client communications in Bulgarian law may create conflicts with different privilege standards in other Member States.
- **Evidence Admissibility Standards**: The strict requirements established by Bulgarian courts for the admissibility of telecommunications evidence may not align with more flexible standards in other jurisdictions.

These challenges underscore the need for significant legal reforms in Bulgaria to ensure effective participation in cross-border judicial cooperation while maintaining adequate protection of fundamental rights. The ongoing legislative reforms following CJEU and ECtHR rulings demonstrate Bulgaria's commitment to addressing these issues, but substantial work remains to achieve full compatibility with European standards for cross-border cooperation in telecommunications interception cases.

7.3.3 Poland

7.3.3.1 Use of Telecommunications Interception in Jurisprudence

Polish jurisprudence establishes clear parameters for the legitimate use of telecommunications interception in criminal proceedings. The **Judgment of the Court of Appeal in Wrocław (2015, ref. no. II AKa 292/15)** demonstrates that operational surveillance must meet specific technical and legal requirements under Article 19(7)(4) of the Police Act. The court ruled that specifying particular telephone numbers as surveillance targets satisfies legal requirements, even when the users' identities remain unknown to law enforcement. This pragmatic approach recognises that telecommunications interception serves primarily to establish perpetrator identity and gather criminal evidence.

The **Judgment of the Court of Appeal in Poznań (2020, ref. no. IV Ka 445/20)** further confirms the necessity of proper judicial authorisation from competent district courts. The court validated wiretapping conducted based on decisions from district courts in Poznań and Warsaw, which had ordered operational surveillance, including the acquisition and recording of conversation content through telecommunications networks and electronic correspondence. This case establishes that when proper procedural requirements are met, telecommunications interception evidence is admissible in criminal proceedings.

7.3.3.1.1 Catalogue of Qualifying Offences and Proportionality

A fundamental principle emerging from Polish case law is the restrictive application of telecommunications interception to specific categories of crimes. The **Judgment of the Court of Appeal in Wrocław (2015, ref. no. II AKa 292/15)** and the **Decision of the Court of Appeal in Poznań (2020, ref. no. II AKz 613/19)** both emphasise that materials obtained through operational surveillance can only be used as evidence in cases concerning offences listed in the statutory catalogue justifying such surveillance measures.

The Poznań court specifically ruled that evidence obtained from wiretaps concerning fraud against property of ordinary value was inadmissible because such offences fall outside the prescribed

catalogue. This restrictive approach reflects the principle of proportionality, ensuring that intrusive surveillance measures are reserved for sufficiently serious crimes that justify the interference with fundamental rights.

7.3.3.1.2 Safeguards and Procedural Protections

Polish jurisprudence demonstrates a strong commitment to procedural safeguards in telecommunications interception. The **Judgment of the Court of Appeal in Poznań (2020, ref. no. IV Ka 445/20)** explicitly linked procedural compliance with fundamental rights protection, stating that basing the entire trial on illegally obtained evidence violates the right to a fair trial under Article 6(1) of the ECHR.

The concept of 'subsequent consent' introduced in Polish law provides an additional safeguard mechanism. The **Judgment of the Court of Appeal in Katowice (2013, ref. no. II AKa 46/13)** explained that when operational surveillance exceeds the original court authorisation, subsequent judicial consent is required to use any evidence obtained beyond the initial scope. This mechanism balances the need to preserve potentially valuable evidence with the requirement for judicial oversight.

Challenges for EIO and Cross-Border Cooperation:

- **Catalogue Incompatibility**: Poland's restrictive catalogue of qualifying offences may not align with broader catalogues in other Member States, potentially causing refusal of EIO requests for telecommunications interception.
- **Proportionality Assessment Divergence**: Polish courts' detailed proportionality reviews may conflict with issuing states where proportionality is presumed once judicial authorisation is granted.
- **Subsequent Consent Mechanism**: Other Member States lacking similar retrospective authorisation procedures may find Polish evidence inadmissible or vice versa.
- **Technical Specification Requirements**: Polish emphasis on precise technical details (telephone numbers, interception methods) may exceed standard EIO form requirements, necessitating additional documentation.

7.3.3.2 Use of Evidence Obtained Abroad

7.3.3.2.1 Mutual Legal Assistance Framework

Polish courts have addressed the admissibility of telecommunications evidence obtained through international cooperation mechanisms. The **Decision of the Court of Appeal in Poznań (2020, ref. no. II AKz 613/19)** established that evidence obtained from foreign sources must comply with both Article 20 of the Convention on Mutual Assistance in Criminal Matters and Article 237 § 3 of the Code of Criminal Procedure.

This dual compliance requirement ensures that evidence obtained through cross-border cooperation meets both international legal standards and domestic procedural requirements. The court's emphasis on strict compliance with international instruments reflects Poland's commitment to maintaining high standards in mutual legal assistance while protecting fundamental rights.

7.3.3.2.2 Admissibility Standards for Foreign Evidence

The **Judgment of the Court of Appeal in Warsaw (ref. no. II AKa 33/18)** addressed procedural requirements in EIO execution, emphasising that formal compliance with international cooperation procedures is essential for evidence admissibility. While this case dealt primarily with procedural issues rather than telecommunications interception specifically, it establishes the principle that procedural violations in cross-border cooperation can result in evidence exclusion. Polish jurisprudence consistently applies the principle that cross-border evidence must meet the same procedural standards as domestic evidence. The courts have made clear that the international nature of evidence collection cannot be used to circumvent domestic procedural safeguards or fundamental rights protections.

7.3.3.2.3 Third-Party Protection in Cross-Border Context

The **Supreme Court ruling (2015, ref. no. I NSNk 6/20)** examined the use of evidence obtained during operational investigations against persons not originally targeted. The court established that evidence gathered through operational surveillance can only be used against third parties with subsequent court consent, a principle with particular relevance for cross-border cases where surveillance may inadvertently capture communications of individuals in other jurisdictions.

This safeguard ensures that the rights of individuals not originally targeted by surveillance are protected through proper judicial oversight, regardless of whether the surveillance was conducted domestically or through international cooperation.

Challenges for EIO and Cross-Border Cooperation:

- **Dual Compliance Burden**: Evidence must satisfy procedural requirements of both issuing and executing states, creating potential for double jeopardy where standards conflict.
- **Fundamental Rights Protection**: Courts may invoke fundamental rights protections to refuse cross-border evidence that fails to meet constitutional standards.
- **European Standards Compliance**: Evidence obtained through systems not meeting ECtHR standards may face admissibility challenges in cross-border proceedings.
- **Judicial Review Standards**: Different levels of judicial oversight across Member States may undermine mutual trust in evidence sharing.
- **Procedural Equivalence Assessment**: Determining whether foreign procedures provide equivalent protection to Polish standards requires detailed case-by-case analysis.
- **Third-Party Rights Protection**: Evidence involving non-suspects may require additional authorisation procedures not anticipated in standard EIO processes.
- **Evidence Exclusion Rules**: Polish courts' strict approach to evidence exclusion may result in the rejection of foreign evidence that would be admissible in the issuing state.
- **Technical Standards Divergence**: Different national approaches to telecommunications interception may create compatibility issues in cross-border evidence sharing.
- **Notification Requirements**: Divergent approaches to post-surveillance notification may create conflicts in international cooperation.

7.3.3.3 Synthesis: Implications for Cross-Border Judicial Cooperation

The Polish jurisprudence on telecommunications interception underscores that effective cross-border cooperation via the European Investigation Order requires harmonisation of substantive and procedural standards, mutual trust in judicial oversight, and technical interoperability:

1. **Procedural Equivalence:** Polish courts insist that interception measures adhere to stringent authorisation, specificity, and proportionality requirements (**Wrocław II AKa 292/15; Poznań IV Ka 445/20**). To facilitate EIO execution, issuing states must demonstrate that their legal frameworks provide safeguards equivalent to Poland's, ensuring decisions will be recognised without protracted verification.
2. **Catalogue Alignment:** The narrow Polish catalogue of qualifying offences (**Poznań II AKz 613/19**) often diverges from broader lists in other Member States. Cross-border interception requests should be limited to offences common to both jurisdictions, or accompanied by legal assurances that evidence will be used only for catalogue-compliant crimes.
3. **Subsequent Consent and Third-Party Protections:** Poland's 'subsequent consent' mechanism (**Katowice II AKa 46/13; Supreme Court I NSNk 6/20**) protects non-targets and retroactively validates over-broad taps. EIO requests must clarify how partner states address incidental interceptions and ensure comparable remedies are available to avoid evidence exclusion.
4. **Dual-Legality and Evidence Admissibility:** Evidence obtained abroad must meet both the issuing state's rules and Poland's procedural safeguards (**Poznań II AKz 613/19**). Issuing authorities should provide detailed documentation of foreign interception authorisations and demonstrate that fundamental-rights protections (fair-trial guarantees) are equivalent, avoiding dual-legality conflicts.
5. **Technical Granularity:** Polish courts require precise technical details (target numbers, interception methods) often exceeding Annex C of the EIO form (**Warsaw II AKa 33/18**). Supplementary technical annexes and explanatory notes should accompany EIOs to ensure executing courts have the necessary information for lawful implementation.

By addressing these areas – procedural equivalence, catalogue harmonisation, retrospective safeguards, dual-legality compliance, and technical specificity – Member States can strengthen mutual trust, reduce refusals, and enhance the admissibility of telecommunications interception evidence obtained under the EIO framework.

8. CHALLENGES AND BEST PRACTICES IN CROSS-BORDER INTERCEPTION OF TELECOMMUNICATIONS IN THE EUROPEAN UNION

As highlighted in Section 6, since 22 May 2017, the EIO Directive has served as the EU's core legal instrument for cross-border evidence gathering through various investigative measures, including covert measures such as the interception of telecommunications.[293] In their 2019 *Joint Note on the practical application of the EIO*,[294] Eurojust and the European Judicial Network (EJN) identified a range of challenges, along with examples of both best and worst practices related to the Directive's implementation. These challenges, *inter alia*, include issues concerning the scope of the EIO, the designation of competent authorities, the content, form, and language of EIOs, as well as difficulties arising during the four main phases of an EIO's lifecycle: issuance, transmission, recognition, and execution. The Joint Note also draws attention to particular challenges associated with specific investigative measures.

Another key EIO-related document is Eurojust's *Report on Casework in the Field of the EIO*, which was previously referenced in the section on the EU framework. The report is primarily based on an analysis of EIO-related cases registered at Eurojust between May 2017 and May 2019. In addition to case-based findings, it includes the results of five operational topics initiated by National Desks, each focusing on specific aspects of the EIO.[295]

This section summarises the key points from both documents regarding the interception of telecommunications. It examines the main challenges and obstacles encountered in the practical implementation of the EIO in cases involving telecommunications interception, and it also highlights additional issues identified by the authors of this report that are not covered in the aforementioned documents.

8.1 The scope of the EIO Directive and the meaning and scope of 'interception of telecommunication'

Article 3 of the EIO Directive on the scope of the EIO refers to 'any investigative measure,' with the exception of the setting up of a joint investigation team (JIT). According to Eurojust and the EJN, the following criteria could be helpful in assessing whether the EIO Directive should apply: (a) the order concerns an investigative measure to gather or use evidence, (b) the measure was issued or validated by a judicial authority, and (c) the measure relates to Member States bound by the EIO Directive.[296] Given this broad scope, the *EIO Directive applies to all investigative measures provided that the purpose of the requested measures is to gather evidence and that a judicial authority of a Member State has issued or validated them*.

The EIO Directive does not define the term 'telecommunications' – neither in the preamble, nor in Article 2 (Definitions), nor in Articles 30–31 (Interception of telecommunications). It also does not refer to the laws of Member States for its interpretation. In the absence of a normative definition and a preliminary ruling by the CJEU on this issue, the precise meaning of the term remains

[293] Pursuant to Article 34(1), the Directive replaced the corresponding provisions of the Mutual Legal Assistance (MLA) Conventions, including the 1959 Council of Europe Convention and its two Additional Protocols, as well as the 2000 MLA Convention.
[294] See n. 4.
[295] See n 6, p. 5.
[296] See n 4, pp. 5-6.

uncertain. This lack of definition creates legal ambiguity, particularly when interpreting Articles 30 and 31.[297]

Older EU instruments, such as the 1995 Council Resolution on the lawful interception of telecommunications and the 2000 MLA Convention, support a broad interpretation of the term, encompassing all existing and future telecommunications technologies. Specifically, the Council Resolution defines telecommunications as:

'any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic, or photo-optical system.'[298]

In contrast, the Convention itself does not define the term. However, the explanatory report to the Convention states that it should be understood '*in the widest sense of the word*,' and affirms that, due to the absence of a precise definition, the provisions on the interception of telecommunications are intended to apply to all forms of communication enabled by current and future technologies.[299]

Nevertheless, the explanatory report acknowledges that, at the time of drafting, it was impossible to foresee every hypothetical scenario due to the rapid pace of technological advancement in this field. While the report advocates for a broad interpretation of the term to include future telecommunications technologies, it still presupposes the involvement of some form of technological means to facilitate communication. In other words, the term 'telecommunication' – as distinct from the broader term 'communication' – does not appear to encompass direct, face-to-face interactions between individuals that occur without the aid of any technological device. From a strictly literal standpoint, this would exclude situations such as two people conversing in a room or having a direct conversation inside a car without any form of transmission technology.[300]

While the absence of a definition and CJEU case law leaves room for ambiguity, the prevailing view, according to Eurojust, is that national authorities should interpret relevant laws in a manner that supports the purpose and effectiveness of EU law, in line with the broader objectives of the EIO Directive – particularly the establishment of an area of freedom, security, and justice. From this perspective, Eurojust encourages practitioners to consider the following:

- Scenarios involving cross-border surveillance that do not require the technical assistance of another Member State do not appear to fall within the scope of the general EIO regime – since there is no issuing authority, no executing authority, and no formal 'order' to be executed. Instead, such cases fall under the specific notification regime set out in Article 31 of the EIO Directive.
- Prior authorisations are generally well justified in domestic scenarios, but considerably less so in cross-border contexts, where suspects may cross borders unexpectedly during an interception already authorised ex ante by the judicial authority of another Member State. Article 31 of the EIO Directive acknowledges this reality by allowing for ex post authorisations. This flexibility recognises that a strict and inflexible prohibition on using

[297] See n 6, p. 44.
[298] See n 76.
[299] Explanatory Report on the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union OJ C379/7 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2000_379_R_0007_01 accessed 4 August 2025, p. 7–29. See also n 6, pp. 44-45.
[300] I*bid*.

material intercepted without prior authorisation could undermine the broader objective of establishing an area of freedom, security, and justice. Importantly, even with an ex-post authorisation, the notified authority retains the right to refuse or restrict the use of the intercepted material on other legal grounds.

- In situations where the subject of the interception is located in a Member State from which no technical assistance is required (Article 31), the EIO Directive explicitly permits ex post authorisations. Specifically, the intercepting Member State must notify the competent authority of the notified Member State of the interception either during the interception or immediately after it becomes aware that the subject was, or had been during the interception, present on the territory of the notified Member State.
- There is no indication that the EIO legislature intended to exclude surveillance measures from the scope of the EIO Directive – except for those explicitly covered by Article 40 of the Convention implementing the Schengen Agreement – or from the application of Articles 30–31 of the Directive. Given the Directive's stated objective 'to cover all investigative measures,' it may be argued that the EU legislature intended to address interceptions conducted for the purpose of criminal investigations in a non-restrictive manner, regardless of the specific nature of the interception.
- Although the methods of interception differ – wiretapping involves intercepting communication via telephone or other telecommunication technologies, while bugging entails placing a small microphone in a specific location and transmitting audio to a nearby receiver – both forms of electronic surveillance serve the same purpose and produce the same effect: the covert interception of communications. Consequently, they involve a comparable level of interference with the right to privacy. It would therefore be illogical for the safeguards and rights established by the EU legislature to apply to the former but not to the latter or to other, potentially more intrusive, measures.
- Eurojust further highlights that, from a comparative law perspective, there is an additional argument in favour of aligning legal treatment: some jurisdictions, while recognising the distinction between different types of interception (e.g., wiretapping and bugging), nevertheless apply the same legal provisions to both.[301]

In their reference documents, Eurojust and the EJN have not addressed whether, in addition to real-time interception of telecommunications (such as live surveillance and interception of the content of conversations via telephones and other telecommunication means), related measures – commonly found in many national legal systems – also fall under the specific provisions on telecommunications interception or whether they are subject to the general regime of the EIO Directive. Such related measures may include, for example, the real-time interception and transmission of traffic data related to a conversation or the real-time tracking of mobile phone

[301] This appears to be the case in Slovenia, a partner country in the INCEPT project, where the Slovenian Criminal Procedure Act (CPA) clearly distinguishes between the surveillance of telecommunications involving wiretapping and recording with the participation of telecommunications service providers (Article 150, § 1/1), and wiretapping and observation conducted within a dwelling or other private premises using technical means, which may also involve the covert entry of police into such premises (Article 150, § 1/4). Although the CPA makes a clear distinction between these two measures and acknowledges their technical differences, both wiretapping (and other forms of telecommunications interception) and bugging fall under the same regulatory framework. They are governed by the same article and subject to identical issuance conditions, due to their similar purpose and comparable impact on the right to privacy.

locations using IMSI catchers. If the term 'telecommunications interception' is to be understood 'in the widest sense of the word,' then the answer would arguably be affirmative.

In sum, Eurojust acknowledges that, in the absence of clear EU legislation or CJEU case law regarding interception through surveillance devices, it remains difficult to provide definitive guidance on how these provisions should be interpreted. Nevertheless, national authorities, when interpreting national legislation that implements EU law, should do so in a manner that aligns with the objectives of the EIO Directive and EU law more broadly.

To help clarify the interpretation and scope of the EIO Directive, the EJN Secretariat has published a document titled *'Competent Authorities, Languages Accepted, Urgent Matters and Scope of the EIO Directive*,' available on the EJN website.[302]

8.2 Content and form

8.2.1 Filling in the EIO (Annexes A, B and C)

Eurojust and the EJN highlight that, in practice, EIOs are sometimes too brief and lack essential information – such as the rationale for the investigative measure, relevant dates, details about the individuals involved, or a sufficient description of the facts under investigation. These omissions can make it difficult, for example, to assess double criminality. As a result, the consultation procedure is triggered, requiring the issuing authority to provide additional information in accordance with Article 11(4) of the EIO Directive.

Confusion and delays may also be caused because the wording used in the Annexes to the national laws transposing the EIO Directive does not always fully correspond to the wording used in the official EIO Annexes. Further difficulties may also occur if several persons are concerned or if multiple competent authorities at the regional level are involved in the executing Member State, and if multiple measures are requested.

Given the potential difficulties that may arise when issuing or executing an EIO – including cases involving the interception of telecommunications or other coercive measures – the information provided in Annexes A, B and C should be specific and detailed, as EIOs typically do not include supporting documents. Practitioners should clearly outline the reasons for issuing the EIO in the particular case and specify what is expected to be heard, discovered, or achieved through the execution of the requested measures.[303]

8.2.2 Information or documents to be – or not to be – provided by the issuing authority

Even though Article 5 EIO Directive on the content and form of the EIO does not impose any legal requirement for the domestic judicial decision to be mentioned or attached to the EIO, some countries do require, under their national law, the attachment to the EIO of a domestic order by the issuing State. According to Eurojust and the EJN, in the event of a request for interception of telecommunications (as well as for other covert investigative measures), pragmatic solutions need

[302] European Judicial Network, 'Competent authorities, languages accepted, urgent matters and scope of the EIO Directive' (6 March 2020) https://www.ejn-crimjust.europa.eu/ejnupload/DynamicPages/Competent%20authorities-languages%20accepted-scope-6%20March%202020.pdf accessed 4 August 2025.
[303] See n 4, p. 7.

to be applied, such as keeping the EIO simple and attaching the (lengthier) domestic order, with or without a translation.[304]

8.2.3 Language

According to Article 5(3) of the EIO Directive, '*the competent authority of the issuing State shall translate the EIO set out in Annex A into an official language of the executing State or any other language indicated by the executing State*.' Regarding issuing and executing the EIOs, the Joint Note identifies several language and translation-related issues and challenges. The recommendations provided by Eurojust and the EJN in this regard should be understood as applicable for all investigative measures, including telecommunications interception.

Some Member States have indicated, despite the wording of the EIO Directive, that they will only accept their own official language, or that they will only accept English in urgent cases. This can be considered a bad practice which significantly hinders the effective execution of the EIOs and the cross-border collection of evidence.[305]

Eurojust and the EJN emphasise that the EIO is a judicial order and, as such, must be issued in the language(s) of the issuing Member State. Only the sections of the form completed by the issuing authority should be translated by the executing Member State to prevent the risk of unofficial or inaccurate translations. If an EIO is not provided in the language of the issuing Member State, the executing authority cannot translate the unclear parts of the request domestically.[306]

8.3 Issuing and transmitting

8.3.1 Issuing and validating authority (verifying an incoming EIO on telecommunications interception)

Article 2(c) of the EIO Directive requires that EIOs be issued or validated by a judge, a court, an investigating judge, or a public prosecutor competent in the case concerned. Central authorities may only play a supporting administrative role in assisting the judicial authorities. With regard to verifying whether the issuing or validating authority of an EIO is competent, executing authorities typically rely on the principle of mutual trust. As with accepted languages and translations, when assessing whether an incoming EIO for the interception of telecommunications or any other investigative measure has been issued or validated by a competent authority of another Member State, the EJN document entitled *'Competent authorities, languages accepted, urgent matters and scope of the EIO Directive'* may serve as a helpful reference.[307]

8.3.2 Proportionality check, consultation mechanism, and costs

The EIO Directive leaves the proportionality check (i.e. establishing whether the required interception of telecommunication or any other measure is necessary and proportionate in a given case) in the hands of the issuing authority (Article 6(1)). The issuing Member State must also

[304] *Ibid*., p. 8.
[305] *Ibid*., p. 9.
[306] *Ibid*. The EIO forms (Annexes A, B and C) are available in all EU languages in Word format in the judicial library on the EJN website. Additionally, the Compendium tool on the EJN website offers an automatic translation function of the 'static' parts of the form. Useful information on accepted languages, including in urgent cases, is also provided by the EJN document in n 302.
[307] *Ibid*., 186.

check whether the measure (telecommunication interception, for example) could have been ordered under the same conditions in a similar domestic case. Here, both the issuing and executing authority can rely on the consultation mechanism to provide relevant information, clarify the description of the offence, describe the requested measure more precisely and to avoid the risk that execution is further delayed. After consultation, the issuing authority may still decide to withdraw the EIO.[308]

The consultation mechanism may also be used to resolve cases – including those involving telecommunications interception – where the associated costs are considered 'exceptionally high'.[309]

8.3.3 Multiple measures

When in addition to the interception of telecommunications other investigative measures are requested, they should, in principle, be included in one EIO. However, in certain situations, Eurojust and the EJN propose a different approach depending on the nature and scope of a case.

When requesting multiple measures, it may be preferable to issue a separate EIO for the interception of telecommunications to avoid disclosing certain information to suspects, which could jeopardise the execution of the measures.[310]

Issuing several EIOs instead of a single one may also be more appropriate in complex cases where telecommunications interception and several other investigative measures are required for different natural or legal persons who hold varying roles in the proceedings. In such situations, maintaining consistency across the various sections of Annex A is a common concern among practitioners.[311]

Finally, multiple EIOs may be necessary when different authorities are responsible for executing telecommunications interception, either independently or alongside other measures. However, some countries view this as an internal matter, arguing that the executing Member State should manage the distribution of tasks rather than requiring separate EIOs.[312]

8.3.4 Transmission

In addition to direct communication between the Member States' competent authorities themselves, different channels are used to secure speedy and safe transmission of EIOs and ensure authenticity.

A *Secure Online Portal* for exchanging e-evidence has been developed by the European Commission. This platform provides a secure communication channel for the digital exchange of

[308] See n 4, p. 10.
[309] *Ibid.*
[310] *Ibid.*
[311] *Ibid.*
[312] *Ibid.*

European Investigation Orders (EIOs) and corresponding replies between EU judicial authorities.[313]

Additionally, EIOs – including those requesting telecommunications interception – can be transmitted via the secure telecommunication connections of *Eurojust* and the *EJN* (see Article 7(4) of the EIO Directive).[314] Eurojust and the EJN can provide facilitation and guidance throughout the various phases of the EIO life cycle, including drafting, transmission, recognition, execution, and follow-up. Where differences between national laws complicate direct cooperation among national authorities, they can give support in clarifying these differences and finding solutions acceptable to both the issuing and the executing authorities.[315] Whenever a consultation procedure is triggered or whenever additional feedback is needed, they can play the role of bridge-maker. To determine whether to contact Eurojust or the EJN in a specific case involving telecommunications interception, practitioners may consult the '*Joint Paper – Assistance in International Cooperation in Criminal Matters for Practitioners: EJN and Eurojust.*'[316]

8.4 Recognition and execution

8.4.1 Competent authorities

Eurojust and the EJN recognised as best practice the fact that some Member States have created a centralised receiving authority, i.e. a judicial authority that receives and, if competent, recognises the EIO and afterwards allocates it for execution to the competent executing authority.[317]

If the executing Member State has no central receiving authority, the issuing authority should make the respective executing authorities aware of the existence of the multiple measures requested within the country.[318] For the identification of the competent executing authority and the relevant contact details, the EJN Atlas can be consulted.[319]

8.4.2 Recognition and execution

Execution is governed by the law of the executing Member State. However, since the executing authority must recognise an EIO 'without any further formality required' and ensure its execution (Article 9(1) EIO Directive), a detailed examination of the file is not permitted in the executing State. The EIO for telecommunications interception, or any other investigative measure, should be carried out 'in the same way and under the same modalities as if the investigative measure had been ordered by an authority of the executing Member State.' Nevertheless, the executing

[313] *Ibid*., pp. 10-11.
[314] *Ibid*., p. 11.
[315] See n 6, p. 11.
[316] European Judicial Network, 'Joint Paper on Assistance in International Cooperation in Criminal Matters for Practitioners: What can we do for you?' https://www.eurojust.europa.eu/publication/joint-paper-ejn-ej-assistance-international-cooperation-criminal-matters-practitioners accessed 2 August 2025.
[317] See n 4, p. 11.
[318] *Ibid*.
[319] European Judicial Network, 'Judicial Atlas' https://www.ejn-crimjust.europa.eu/Ejn2021/AtlasChooseCountry/EN accessed 2 August 2025.

authorities should comply, as far as possible, with the formalities and procedures expressly indicated by the issuing authorities – provided these are not contrary to the fundamental principles of law in the executing State (Article 9(2)).[320]

8.4.3 Differences in national legal frameworks

Differences in national legal frameworks may hinder effective cooperation among national authorities at any stage of the EIO life cycle, posing a significant challenge to cross-border evidence gathering through the EIO mechanism.[321]

The overview of relevant legal provisions on the interception of telecommunications in the four countries participating in the INCEPT project (see Section 6 of this report) revealed significant differences across several key areas. While certain legal concepts and solutions are shared by all countries, their national frameworks for telecommunications interception and other covert investigative measures vary notably. These variations include differences in definitions, types and technical solutions, competent authorities, lists or categories of offences for which interception is permitted, thresholds and prerequisites for judicial authorisation, time limits and duration rules, oversight mechanisms, and the admissibility and use of evidence.

Discrepancies in national frameworks are considerably smaller when it comes to the protection of communication privacy and other fundamental rights. However, in practice, national authorities may interpret EU and international human rights standards quite differently.

More particularly, in the four countries, there are varying degrees of difference in the terminology used to define measures related to telecommunications interception. For instance, Polish legislation does not use terms such as 'interception' or 'surveillance'. Each country's legal framework employs different wording to describe the types of measures and the prerequisites for their implementation. In all countries except Slovenia, intelligence agencies are authorised to intercept telecommunications, and the materials they obtain may be used in criminal investigations and proceedings. In this regard, Bulgaria stands out, as its State Agency for National Security (SANS) is authorised to intercept telecommunications based on internal approval and extensions, without stringent judicial oversight.

Notably, while none of the four countries has an explicit legal basis for ‘Trojan horse’ surveillance, such practices may be used in practice in Bulgaria and the Czech Republik, while they are are not permitted in Slovenia and Poland. This may be due, at least in part, to the absence of a common EU regulatory framework on interception – particularly regarding the technical means of execution – as well as the lack of definitive guidance from the CJEU and ECtHR case law.

Nevertheless – and perhaps most importantly – in all four countries, telecommunications interception is considered a special or covered measure that significantly interferes with individuals’ fundamental rights. As such, it requires judicial authorisation, must meet specific legal thresholds, is restricted to the investigation of serious crimes, and is subject to strict time limitations and oversight by courts and other supervisory bodies.

Table 7: Interception of telecommunications – similarities and differences between countries

	SLOVENIA	BULGARIA	CZECH REP.	POLAND

[320] See n 4, pp. 11-12.
[321] See n 6, p. 22.

Definitions, types and technical solutions	covered investigative measures (CIM) wiretapping and recording; surveillance of all forms of electronic communications; real-time preservation and transmission of communications traffic and location data; access to stored communications traffic and location data use of IMSI catchers (may be used solely for tracking the location of a device); Trojan horse surveillance (lacks legal basis; it cannot be used) materials obtained by Security Agency (SOVA) and Intelligence and Security Service of the Ministry of Defence (OVS MORS) cannot be used in criminal investigations/ proceedings	Special Intelligence Means (SIM) wiretapping/eavesdropping; real-time interception of the content of telephone and internet communications; traffic and location data collection regarding telecommunications; use of IMSI catchers (not explicitly regulated; may be used under general provisions on SIM); Trojan horse surveillance (not explicitly regulated; may be used under general provisions on SIM) State Agency for National Security (SANS) can intercept telecommunications with its own authorisation and materials obtained by them can be used in criminal investigations involving national security issues	covert investigative measures (CIM) wiretapping; interception of electronic communications; access to stored communications metadata; surveillance of persons and objects (incl. collection of stored communication content); freezing of stored data use of IMSI catchers (not explicitly regulated; may be used under general provisions on CIM) Trojan horse surveillance (not explicitly regulated; may be used under general provisions on CIM) intelligence agencies can intercept telecommunications and materials obtained by them can be used in criminal investigations/proceedings	**different statutes introduce varying terminology for covert investigative measures* **there are two parallel systems: procedural surveillance based on CCP and extra-procedural (e.g., operational) surveillance based on other statutes* obtaining and recording the content of conversations conducted using technical means (incl. telecommunications networks); obtaining and recording the content of correspondence (incl. correspondence transmitted via electronic communication); obtaining and recording communication data contained in data storage media, telecommunications terminal devices, and IT and ICT systems use of IMSI catchers (not explicitly regulated; their use appears to be permitted as a form of 'technical means' authorised under specific statutes); Trojan horse surveillance (lacks a clear legal basis; under the currently binding law, it should not be used) agencies or entities other than the police (such as the Border Guard, Military Gendarmerie, Central Anti-Corruption Bureau, National Revenue Administration, and Internal Security Agency) can intercept telecommunications and materials obtained by them can be used in criminal

				investigations/proceedings in limited cases
Competent authorities	investigating judge	Court	court	court (CCP: on a request of a prosecutor; special statutes: on a request of the police, or other LEAs after a consent of the Prosecutor General)
Offences	catalogued criminal offences and any criminal offence for which a prison sentence of at least eight years is prescribed	catalogued serious crimes committed with intent	offences with higher statutory penalties	catalogued criminal offences (special statutes contain their own catalogues which differ from the one provided in the CCP)
Thresholds and prerequisites	reasonable grounds for suspicion reasonable suspicion that a particular means of communication is being used; reasonable conclusion that the location of the perpetrator cannot be determined by other measures, or that doing so would involve disproportionate difficulty principle of proportionality (not explicitly articulated in the CPA)	grounds for suspicion when relevant circumstances cannot be established in any other way or it would involve extreme difficulties; when less intrusive methods are insufficient	necessity and proportionality (in relation to the seriousness of the offence); inadequacy of existing evidence-gathering methods	**prerequisites vary depending on whether the interception is carried out under the provisions of the CCP or under special statutes* CCP: a justified suspicion/concern; special statutes: ineffectiveness or unsuitability of other means for conducting operational and investigative activities; the purpose of identification, prevention, and detection of catalogues offences, as well as the identification of perpetrators and the acquisition and preservation of evidence; principle of proportionality (not explicitly articulated in the statutes)
Time limits	max. 6 months; IMSI catchers max. 1 month	max. 6 months (except in terrorism cases); no strict time limit for SANS	max. 4 months; surveillance of persons and objects max. 6 months	max. 6 months

In practice, differences between countries may arise in cases where telecommunications interception is carried out without the technical assistance of the notified Member State. While Article 31 of the EIO Directive requires the notified state to verify whether such interception would be lawful under its own domestic law, Member States vary in how strictly they interpret this obligation – some conduct only a formal review, while others assess substantive legality, which may result in delays or even the blocking of the interception.[322]

[322] As no such differences have been identified among the participating countries (see Section 6), this issue should be further explored in later stages of the project.

8.4.4 Recourse to a different type of investigative measure

To address such situations, the EIO Directive assigns the **proportionality check** to the issuing authority. However, it also allows the executing authority to invoke grounds for non-recognition or non-execution (see below) or to *resort to an alternative investigative measure if it would achieve the same result through less intrusive means* (Article 10(3)). In their Joint Note, Eurojust and the EJN emphasise that, to avoid unnecessary consultations and delays between executing and issuing authorities, the latter *should indicate in the EIO whether less intrusive measures – capable of achieving the same result – could be considered*.[323]

8.4.5 Incompatibility with the obligations regarding fundamental rights and other grounds for non-recognition or non-execution

Pursuant to Article 11(1)(f) of the EIO Directive, recognition or execution of an EIO may be refused by the executing State if the latter would have had substantial grounds to believe that the execution of the investigative measure indicated in the EIO would be incompatible with fundamental rights (e.g., with its 'obligations in accordance with Article 6 TEU and the Charter').

Surprisingly, the cases analysed by Eurojust for its report did not include any instance in which the executing authority invoked substantive grounds to believe that executing the EIO would be incompatible with its obligation to respect and protect fundamental rights, as enshrined in the Charter of Fundamental Rights of the European Union and referenced in Article 6 TEU. Although differences between national legal systems occasionally gave rise to discussions concerning fundamental rights, these discussions did not relate to the interception of telecommunications.[324]

Overall, Eurojust and the EJN call for a restrictive interpretation of the grounds for non-recognition set out in Article 11 of the EIO Directive. Since these grounds – as well as those in Chapter IV of the Directive – are listed exhaustively, there is no room to refuse the execution of EIOs based on grounds not included in this list, such as the principle of opportunity.

Drawing on Recital 20, the Joint Note indicates that 'immunities or privileges' that may render the execution of an EIO impossible can include protections afforded to the medical and legal professions. They may also encompass, even if not immunities or privileges in the strict sense, rules relating to freedom of the press and freedom of expression.

The Joint Note also advises practitioners to consider Article 11(4) of the EIO Directive, which establishes an *obligation for the executing authority to consult the issuing authority in relation to most grounds for non-recognition before deciding not to recognise or execute an EIO*.

Such a situation could hypothetically arise if a Member State issued an EIO requesting the interception of encrypted telecommunications using Trojan horse software, while the executing State – unlike the issuing State – either prohibits the use of such technology or lacks an adequate legal basis for it (Slovenia is an example of such a Member State). In this case, the executing authority would appear to have two options. While consulting with the issuing authority, it could

[323] See n 4, p. 12.
[324] One case referenced in Eurojust's report involved the hearing of a person as a witness who could potentially become a suspect in the same proceedings. The executing authority expressed concerns regarding the right to a fair trial, specifically the privilege against self-incrimination. With Eurojust's assistance, it became clear that the perceived obstacle did not stem directly from Article 6 TEU and/or the Charter of Fundamental Rights, but rather from differences in how the national legal systems of the two Member States interpreted and applied a core fundamental right – both in ways that were nonetheless compliant with the Charter. Ultimately, the European Investigation Order (EIO) was executed successfully. See n 6, p. 36.

either: (a) invoke grounds for non-recognition or non-execution by arguing that the requested investigative measure would not be authorised under their national law in a similar domestic case (Article 11(1)), or (b) propose an alternative investigative measure (if) capable of achieving the same result (Article 10(3)). In practice, the executing authority would likely choose the first option and refuse to recognise or execute the EIO, given that the use of Trojan horse software or similar technologies is, as practical examples suggest, currently the only effective method for intercepting encrypted communications.

8.4.6 Challenges and best practices in urgent cases

Eurojust and the EJN highlight that in urgent cases, fulfilling the formal requirements can be particularly challenging, especially given that the EIO Directive does not provide for provisional measures to be taken before an EIO is formally issued. According to them, Article 7 of the 2000 MLA Convention on the spontaneous exchange of information may offer a solution in certain situations – requests made via email, fax, or even telephone could be accepted before the formal EIO is transmitted. Alternatively, prompt communication with the executing authority through Eurojust or the EJN contact points is recommended to assess available options.[325]

Further best practices identified and proposed by the Joint Note, applicable to any investigative measure, including the interception of telecommunications, include:

- Member States may accept an urgent EIO in English, even if they have not officially indicated acceptance of English or another language under Article 5(2) of the EIO Directive.
- When validation of an EIO is required, Member States may be willing to take initial steps to secure evidence before receiving the validated EIO. In such cases, an email is required, accompanied by a brief written summary of the facts.[326]

More detailed information on urgent matters can be found in the aforementioned EJN document, '*Competent authorities, languages accepted, urgent matters and scope of the EIO Directive.*'[327]

8.4.7 Acknowledgement of receipt and time limits

Regarding time limits for recognition or execution of the EIO and for carrying out investigative measure/s (see Article 12), the Joint note addresses situations where the execution of the EIO is postponed, i.e. situations where pursuant to Article 12(6) the executing authority is unable to meet the time limit and shall inform the issuing authority of the reasons for the delay and consult with it about the appropriate timing to carry out the investigative measure (communications interception, for example). According to Eurojust and the EJN, under no circumstances should the delay be the cause or reason for non-execution.[328]

Early coordination between judicial authorities is essential in cases involving e-evidence and short data retention periods. Article 32 of the EIO Directive provides for the possibility of a so-called provisional measure in very urgent situations, aimed at preventing the destruction, alteration,

[325] *Ibid.*, p. 13.
[326] *Ibid.*
[327] See n 302.
[328] See n 4, p. 13.

removal, transfer, or disposal of an item (including data) that may be used as evidence. The executing authority must decide on and communicate the decision regarding the provisional measure as soon as possible and, where practicable, within 24 hours.[329]

8.4.8 Rule of speciality

The 'rule of speciality' in EU law traditionally applies to extradition and the transfer of sentenced persons. The EIO Directive does not explicitly address this rule, so it is not surprising that Member States hold differing views on whether it applies in the context of issuing and executing EIOs.

When executing an EIO, some Member States specify that the evidence obtained – including that acquired through telecommunications interception – may only be used for the specific investigation for which it was requested. Other executing Member States do not explicitly state this limitation but operate under the assumption that the evidence will not be used for other purposes.[330]

From the perspective of issuing Member States, views also differ: some believe that permission must always be sought from the executing Member State before the evidence can be used in a different case. Others take the position that such permission is not required, as the issuing authority determines the use of the evidence, which may be transferred in accordance with the applicable legal framework on data protection.[331]

Eurojust and the EJN recommend that the issuing Member State submit a separate request before using evidence for purposes other than those stated in the original EIO. Furthermore, in cases where both a Joint Investigation Team (JIT) and an EIO are applied in parallel, they advise that the EIO should explicitly state that the evidence obtained may be shared with members of the JIT[332]

8.4.9 EIO and cross-border surveillance

While, in principle, the EIO Directive does not apply to cross-border surveillance as referred to in the Convention implementing the Schengen Agreement (see Recital 9), some Member States clearly consider such surveillance a matter of judicial cooperation falling within the scope of the EIO regime – particularly when device monitoring, geolocation, and/or wiretapping are involved.[333]

8.5 Challenges related to specific provisions on interception of telecommunications (Articles 30 and 31)

8.5.1 Interception of telecommunications with technical assistance

[329] *Ibid*., p. 14.
[330] *Ibid*., p. 16.
[331] *Ibid*.
[332] *Ibid*. According to Eurojust and the EJN, EIOs and JITs are distinct instruments, and the choice between them should be assessed on a case-by-case basis, depending on the specific circumstances. There is also a possibility to use a combination of both tools if appropriate. Evidence obtained by a JIT member country through an outgoing EIO for the interception of telecommunications addressed to a country outside the JIT can be shared within the JIT, provided the EIO includes an explicit clause permitting such sharing. In countries where enforcement authorities play a significant role, JITs may be the preferred option over the more 'judicialised' EIO framework.
[333] *Ibid*., 17.

In cases involving the interception of telecommunications requiring technical assistance from another EU Member State (Article 30 of the EIO Directive), several recurring challenges have emerged in Eurojust's casework:[334]

- *Insufficient Information*. EIOs often lack key details such as the crime description, proper translation, or the relationship between the intercepted person and the accused. These gaps require clarification via Eurojust on a regular basis.
- *Purpose of Intercepted Material*. In some Member States, disputes have arisen over whether data intercepted by intelligence services can be used as evidence in criminal proceedings, or whether it may be used solely for intelligence purposes. There were cases where executing authorities have approved interception only on the condition that the material be used exclusively for intelligence purposes, as its use as evidence would not be lawful in a comparable domestic case. As shown in Section 6 of this report, despite the absence of a clear legal basis, intelligence agencies in all INCEPT-participating countries – except Slovenia – are permitted to intercept telecommunications, and the materials obtained can be used in criminal investigations and proceedings. In Slovenia, however, the Constitutional Court has ruled that the use of intelligence data in criminal proceedings is prohibited.
- *Authorisation Periods*. Differences in national laws regarding the duration of interception authorisations have caused issues, such as the unexpected termination of interception. Best practice suggests that executing authorities should notify issuing authorities before authorisation expiry to allow timely renewal.
- *Status of the Person*. In at least one case, questions arose about whether it was permissible to intercept communications of someone not formally designated as a suspect, creating legal uncertainty depending on national law.
- *Scope of Interception*. Differing views persist regarding whether Article 30 can be applied to requests involving the installation of a covert listening device in a private space, such as a car, for the purpose of 'bugging' it. Some Member States argued this is beyond the article's scope (see also Sub-section 8.1 of this report).[335]

These issues illustrate the complexity of cross-border cooperation in telecommunications interception and underscore the importance of clear, consistent communication and legal interpretation across Member States.

8.5.2 Interception of telecommunications without technical assistance

Cases where the subject of the interception is located in a Member State from which no technical assistance is required (Article 31, Annex C) highlighted challenges arising from divergent interpretations of Article 31. Issues commonly involved the scope of Article 31, designation of competent authorities and improper or incomplete use of Annex C, including missing details on judicial validation. While some of these issues were addressed by Eurojust and the EJN in their Joint Note, the majority were handled by Eurojust in response to operational topics opened by the National Desks.

One of the issues highlighted by Eurojust and the EJN relates to the ***designation of competent authorities for receiving Annex C***: in some Member States, the central authority is responsible for receiving, while in others, this role is assigned to local authorities.[336]

[334] See n 6, p. 42.
[335] *Ibid*. See also n 4, , p. 15.
[336] See n 4, p. 15.

In some cases, the ***content of Annex C was insufficient*** – either due to a missing description of the crime, an unclear explanation of the relationship between the person subject to interception and the accused, or poor translation that hindered understanding of the circumstances and nature of the offence. Once additional information was provided, consent was usually granted.[337]

Some cases involved the ***interception of communications via bugged vehicles crossing borders***. Authorities sometimes held that such scenarios were not covered by Article 31, or that prior authorisation was required under domestic law. When the Annex C form was submitted after the communication in the car had already occurred, the relevant authority could not approve the use of the evidence.[338]

A key issue which followed from an operational topic opened by the Italian National Desk was the divergence in national approaches to determining ***whether an interception would be authorised in a similar domestic case***. While some notified authorities treated this as a formal procedural check, others conducted a substantive legal assessment – often requesting additional information to complete the evaluation. In some instances, this led to the termination of ongoing interceptions or a prohibition on the use of the intercepted material. Even in cases where such prohibitions were not imposed (e.g., where the use of intercepted material was permitted), the failure to notify or obtain approval still raised concerns about the admissibility of the evidence.[339]

Most National Desks reported that their national legislation had transposed Article 31 of the EIO Directive verbatim. Several National Desks outlined the factors considered by their executing authorities when assessing whether an interception 'would be authorised in a similar domestic case' under national law. These factors included: whether the offence is intentional; whether the information cannot be obtained by other means and is essential to the proceedings; whether the measure interferes with fundamental rights no more than is necessary for the investigation; whether the measure is likely to produce relevant information or evidence; the seriousness of the offence (e.g., in some countries, punishable by at least four or five years of imprisonment); whether the offence constitutes a serious violation of the legal order or is accompanied by other serious offences committed by the suspect; and whether there is sufficient information and legal basis to apply for a court order.[340]

Another issue was ***whether the authorities of the intercepting state have issued guidelines on how the notified state should evaluate Annex C forms***. While several National Desks indicated that such guidelines had been prepared, their content varied. One National Desk explained that its guidelines were intended to assist the judicial authority of the notified state in determining whether the seriousness of the offence would justify interception in a similar domestic case. These guidelines did not address the evidentiary threshold for the interception or the necessity and proportionality of the measure, as those aspects were considered to have already been assessed by the issuing authority. The majority of Member States reported having developed more general guidelines on the implementation of the EIO.[341]

In any case, according to Eurojust and the EJN, national authorities cannot be required to provide more information than what is specified in Annex A. The notification is not a request to recognise

[337] See n 6, p. 44.
[338] *Ibid.*
[339] *Ibid.*, p. 43.
[340] *Ibid.*
[341] *Ibid.*, p. 43-44.

an investigative measure, but rather a formal expression of respect for the sovereignty of the other Member State.[342]

8.6 Other challenges identified by Eurojust and the EJN

8.6.1 The description of the investigative measure requested

Executing authorities sometimes raise questions when they believe that information was missing or wrong in the description of the investigative measure that was requested.

In EIOs related to the interception of telephone calls, in several cases, Eurojust was involved to clarify to the issuing authority the importance of demonstrating the link between the telephone number and the criminal acts, the necessity and proportionality of the requested measure, the suspects involved, the extension of the request and the duration of the requested measure. In other EIOs, information was missing on the place/premises and meetings of the suspect to be intercepted, although this was explicitly required under the law of the executing Member State. Eurojust reports that following its clarifications, most EIOs were successfully executed.[343]

8.6.2 Domestic judicial decision authorising a coercive investigative measure

In cases related to the execution of coercive investigative measures such as a telephone interception, some executing authorities criticised the EIO for lacking an underlying judicial decision authorising the requested measure. Although Article 5 of the EIO Directive does not legally require the attachment of a domestic judicial decision, Eurojust's casework shows that some Member States routinely request it. In most instances, when such decisions were requested, they were translated and provided. One case highlighted a delay due to the omission of Section L of the EIO (regarding the validating judicial authority) and the absence of a court order. Once the domestic court order was submitted, wiretapping was approved within two days.[344]

To streamline future procedures, the executing Member State's National Desk recommended either completing Section L and having it signed by the issuing judge or routinely or ex officio attaching the domestic court order with a translation.

8.6.3 Use of the investigative measure restricted to certain offences

Executing authorities sometimes consult Eurojust when asked to execute EIOs for what they perceive as minor offences. In one case, an EIO requested telecommunications interception, searches, and banking data for a fraud involving only €2,000. The executing authority questioned the proportionality of these measures and considered refusing the EIO under Article 11(1)(h) of the EIO Directive, which allows refusal if such measures are limited to certain offences or thresholds under national law. However, since the requested measures were legally permitted for fraud regardless of the amount involved, the authority ultimately executed the EIO after discussing alternative options with Eurojust.[345]

[342] See n 4, p. 15.
[343] See n 6, p. 24.
[344] *Ibid*., 25.
[345] *Ibid*., 36.

9 ENCROCHAT AND SKY ECC: CROSS-BORDER EVIDENCE GATHERING THROUGH MASS INTERCEPTION OF ENCRYPTED COMMUNICATIONS

While encrypted communications have become essential for protecting privacy in the digital age, they also present significant challenges for law enforcement agencies investigating serious transnational crime, sometimes prompting the use of controversial investigative measures. The **mass interception of telecommunications**, probably the most controversial of all such measures, presents significant legal and ethical challenges, especially regarding the protection of the right to privacy, data protection, and ensuring the right to a fair trial. **EncroChat** and **Sky ECC,** two seminal cases involving high-profile cross-border criminal investigations and the decryption of secure communication platforms used by criminal networks, have brought these issues to the forefront.

9.1 The EncroChat case

EncroChat was a communications service provider offering encrypted smartphones marketed as secure and anonymous. It was allegedly used predominantly by organised criminal groups for illicit activities such as drug trafficking, money laundering, and violent crime. In early 2020, the French police were able, with the technical assistance of Dutch experts and the authorisation of a French court, to infiltrate the EncroChat network and began covert interception of messages.

The investigation in this case marked a turning point in how encrypted services are targeted by law enforcement. It involved large-scale, covert interception and decryption of millions of encrypted messages. The intercepted data was shared in real time with Dutch authorities under a Joint Investigation Team (JIT). Additionally, the German Federal Police Office (Bundeskriminalamt – BKA) was able to retrieve the intercepted data (stored and real-time) relating to EncroChat users in Germany from a Europol server. By means of EIOs, the General Public Prosecution Service of Frankfurt sought ex post authorisation for the transmission and use of these data in German criminal proceedings.[346]

The law enforcement agencies' operation eventually led to thousands of arrests, prosecutions, and convictions in France, the Netherlands, Germany and several other EU countries. Criminal proceedings are still ongoing in certain countries.

A central concern in the EncroChat case is the *lawfulness of the mass interception under national and international law*. The operation involved real-time monitoring without individualised suspicion in many cases, raising questions about proportionality, necessity, and the scope of judicial oversight.[347]

Another major challenge lies in the *admissibility of evidence gathered through such interceptions*. Defendants have argued that the data was obtained unlawfully or without proper disclosure of technical methods.[348]

Courts in different jurisdictions have reached divergent conclusions regarding these challenges. Some, such as in France and the Netherlands, upheld the legality of the operation and admitted

[346] CJEU Communications Directorate, Press Release (April 2024) https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-04/cp240077en.pdf accessed 2 August 2025.
[347] *Ibid*.
[348] *Ibid*.

the evidence. Others, such as certain German courts, initially expressed concerns about the sufficiency of legal grounds and the availability of judicial remedies. The Regional Court of Berlin (*Landgericht Berlin*), one of the courts before which criminal proceedings were brought, submitted a series of questions to the CJEU for a preliminary ruling on the Directive regarding the lawfulness of the EIOs. These questions related to the following issues:[349]

- The German public prosecutor's competence to issue an EIO;
- The admissibility of the EIO pursuant to Art. 6(1) EIO Directive;
- Correct application and interpretation of Art. 31 EIO Directive, which regulates the surveillance of telecommunications without the technical assistance of a Member State;
- The consequences of a possible infringement of EU law for the national criminal proceedings.

The CJEU considered it decisive that the EIO had been issued in order to obtain evidence that was already in the possession of the competent French authorities. The Court noted that the Directive includes a public prosecutor among the authorities, who, like a judge, court, or investigating judge, is understood to be a 'judicial authority' competent to issue EIOs without the necessity of validation.

Considering that the investigative measure indicated in the EIO consisted of obtaining existing evidence already in the possession of the competent authorities of the executing State, the CJEU ruled that the issuing of an EIO is not subject to the same substantive conditions as those that apply in the issuing State in relation to the gathering of that evidence.

Following an explicit question by the Regional Court of Berlin, the CJEU found that the infiltration of terminal devices for the purpose of gathering communication data, as well as traffic or location data from an internet-based communication service, constitutes an 'interception of telecommunications' within the meaning of Article 31(1) of the EIO Directive.

The CJEU also observed that both the wording of Art. 31(1) ('competent authority') and the EIO form leave the question of which authority must be notified open. The intercepting Member State (e.g., France) can submit the notification to any appropriate authority of the notified Member States (e.g., Germany) if it is not able to identify the competent authority in that State. Additionally, the CJEU pointed out that Article 31 intends not only to guarantee respect for the sovereignty of the notified Member State but also to protect the rights of the affected users in that Member State.

Last but not least, referring to Article 14(7) of the EIO Directive, the CJEU clarified that in criminal proceedings national criminal courts are required to disregard information and evidence if the affected person is not in a position to comment effectively on the information and evidence gathered if the information and evidence are likely to have a preponderant influence on the findings of fact.[350]

Obviously, the CJEU allowed German prosecutors to request EncroChat data from France, but it did not go on to say that prosecutors could use the data without approval from a German court. Following the CJEU's decision, a grand chamber of the Berlin Regional Court, made up of five judges, ruled orally in December 2024 that text messages intercepted by French police from the

[349] Case C-670/22 *M.N. (EncroChat)* EU:C:2024:372. See also Wahl T, 'ECJ Ruled in EncroChat Case' (2024) eucrim https://eucrim.eu/news/ecj-ruled-in-encrochat-case/ accessed 3 August 2025.
[350] See CJEU, M.N. (EncroChat), cited above.

EncroChat encrypted phone network cannot be used to prosecute a suspect for alleged drug trafficking offences in Germany.

As a matter of fact, the Court found that French investigators had not intercepted EncroChat data from a central server in France but had harvested it from the handsets of users in German territory. In relation to this, the Court held that the principle of mutual confidence in actions of other member states during judicial cooperation only meant Germany should recognise that France's actions were legal under French law. Under German law, prosecutors were obliged, according to the Berlin Regional Court, to seek approval from the German courts to use the French-supplied data in Germany. The Court assessed that prosecutors had failed to seek judicial approval and that German courts would not have authorised the hacking operation against EncroChat under German law. Prosecutors also had not established that evidence of serious crimes could not have been obtained in a less obtrusive way than by intercepting the data of all EncroChat phone users in Germany.[351]

In another legally significant decision, the Berlin Regional Court found that *French prosecutors failed to comply with European law by failing to follow the correct procedures under EU law to inform Germany of its plans to obtain the phone data of German citizens*. France's *notification should have contained details of the targets identified by phone number, IP address or email, the identity of individuals targeted, as well as a description of the offence committed*.[352]

The Berlin Regional Court also found that the French authorities had not disclosed their communications with German police and that *no information had been supplied to the court on how the data had been intercepted*. This raises *questions over whether defendants had adequate information to challenge the validity of the data*.[353]

A final written version of the decision has yet to be published. Prosecutors are expected to appeal the decision to the Supreme Court in Germany.

The fact that the hacking operation against EncroChat was not merely a French police operation, but rather a joint European initiative involving several other EU Member States, raises the question of whether the decision of the Berlin Regional Court could influence judicial decisions in other participating countries. According to defence lawyers, the answer is yes.

For example, a German defence lawyer maintained that 'the decision would set a precedent for other cases heard in Germany as well as in other countries, though courts elsewhere would make their own decisions on the admissibility of EncroChat evidence.' [354]

A Dutch defence lawyer affirmed that 'the Berlin court's decision could have 'massive' implications for cases in Holland.' She argued that this decision basically confirms defence arguments in the Netherlands. Previously, the Supreme Court rejected his arguments on this point, but along with the Berlin court, even academics are saying that an interpretation like that from the Dutch

[351] Goodwin B, 'German court finds hacked EncroChat phone evidence inadmissible' ComputerWeekly.com https://www.computerweekly.com/news/366617630/German-court-finds-hacked-EncroChat-phone-evidence-inadmissible accessed 2 August 2025.
[352] *Ibid.*
[353] *Ibid.*
[354] See n 351.

Supreme Court can't stand. According to a lawyer from Italy, 'the Berlin court decision was an 'excellent result' but described the legal situation in Italy as 'very complex.'[355]

A lawyer in Montenegro dealing with evidence from police hacking of Sky ECC encrypted phone network, said the EncroChat decision was likely to influence judicial decisions in her country too, and everyone in the judiciary is very keen on what the other countries are doing and how they are dealing with those cases.'[356]

However, recent rulings by various courts, including the Strasbourg Court, have cast serious doubt on these predictions made by lawyers.

Notably, in German judicial practice, the *decision by the Berlin Regional Court is the exception rather than the rule*. Another German regional court found the defendant guilty of ten counts of illicit trafficking of narcotic drugs in significant quantities and sentenced him to an aggregate prison term of five years. To buy and sell the narcotics, the defendant had used an EncroChat mobile device, and the Regional Court based its judgment on an analysis of these data. The defendant's appeal against the conviction was unsuccessful. His defence lawyer objected to both the collection and the use of the EncroChat data as evidence. However, the Federal Court of Justice rejected the appeal on points of law, finding the data obtained and used in this manner to be admissible. Finally, the defendant lodged a constitutional complaint. However, by Order BvR 684/22 of 1 November 2024, the German Federal Constitutional Court declared the complaint inadmissible on the grounds that it failed to meet the procedural requirements of substantiation.[357]

In an *EncroChat-related case that reached the Strasbourg Court*, A.L. and E.J., British nationals, were prosecuted and convicted of conspiracy to illegally import and supply cocaine and heroin, as well as conspiracy to commit three murders and acts of blackmail. Relying on Article 8 of the European Convention on Human Rights (right to respect for private life), the applicants complained to the European Court of Human Rights (ECtHR) about the French authorities' remote retrieval of data from all handsets connected to the EncroChat network and the subsequent transfer of that data to the UK authorities. They challenged both the adequacy of the legal framework governing remote data collection and the necessity of such an interference with their rights. The Court observed that the EncroChat user data had been obtained by the French authorities through a data retrieval measure ordered within the context of a criminal investigation. The data concerning individuals using EncroChat in the UK was then transmitted to the UK authorities as existing evidence in the possession of the French authorities, pursuant to a European Investigation Order (EIO) issued by the UK prosecution service. The ECtHR did not rule on the merits of the case. Instead, it declared the complaint under Article 8 inadmissible on the grounds that the applicants had failed to exhaust domestic remedies. The Court found that an effective remedy had been available to them within the UK legal system.[358]

9.2 The Sky ECC case

[355] *Ibid.*
[356] *Ibid.*
[357] Federal Constitutional Court (Germany), Press Release no 104/2025 (3 December 2024) https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2024/bvg24-104.html accessed 31 July 2025
[358] *AL and EJ v France* App nos 44715/20 and 47930/21 (ECtHR, 17 October 2024)

The Sky ECC case is closely related to the EncroChat case in both nature and legal complexity. Both involve the mass interception of encrypted communications from platforms allegedly used primarily by organised criminal networks. However, there are important differences in timing, technical approach, and legal controversy.

Sky ECC was a secure messaging platform marketed as offering end-to-end encrypted communication and anonymity. It sold modified smartphones with disabled cameras, microphones, and location tracking, making them attractive to criminal users. It had over 100,000 users worldwide; an estimated 70,000 in Europe, with Belgium, the Netherlands, and France among the most affected countries. Authorities claimed that Sky ECC was widely used by criminal organisations for drug trafficking, money laundering, arms dealing, and murder.[359]

In 2021, law enforcement agencies – primarily in Belgium, France, and the Netherlands – infiltrated the encrypted communication system of Sky ECC, capturing millions of messages. This large-scale international criminal investigation required close judicial and law enforcement cooperation. A Joint Investigation Team (JIT) was established between Belgium, France, and the Netherlands, possibly with the participation of other countries as well. Similar to the EncroChat case, the Sky ECC operation involved extensive cross-border exchange of evidence, both in real time and through the transmission of stored telecommunications content. In instances where real-time exchange was not feasible or not covered by the JIT framework, EIOs were used to request or provide evidence. Intercepted data has been shared with prosecutors in Germany, Austria, Spain, and other countries where Sky ECC was reportedly used by organised crime groups.

In Serbia, Bosnia and Herzegovina, Albania, Montenegro and Slovenia, for example, almost 100 people have been arrested and charged as a result of evidence obtained from Sky ECC communications and passed on by the French and Dutch, for crimes involving drug trafficking, murder, and kidnapping.[360]

In Slovenia, a partner country in the INCEPT project, communication data provided by the French police formed the basis for criminal prosecution in two highly publicised cases: ‘Kavaški klan’ and ‘Strojepiska.’ The first case involves the prosecution of members of a Slovenian cell of a Balkan criminal organisation, accused of drug and arms trafficking, kidnappings, and murders. The second case, closely related to the first, concerns criminal proceedings against a former employee of the Specialised State Prosecutor’s Office, who allegedly leaked confidential information – such as planned house searches and arrests – to members of the Kavaški klan. The suspect was identified with the help of communication data transmitted to Slovenian prosecutors by the French police. In both cases, the defence requested the exclusion of the communication data obtained by French law enforcement authorities through the hacking of the encrypted Sky ECC platform. The defence argued that the French police had conducted indiscriminate monitoring of communications and contended that, due to such violations, the resulting evidence could not be used under Slovenian law.[361]

In connection with the Sky ECC investigation, Eurojust facilitated legal coordination, especially in ensuring that the sharing and admissibility of evidence complied with national and EU legal standards, including data protection and fair trial rights. However, like EncroChat, the Sky ECC

[359] Kaymera, 'What happened to Sky ECC' https://blog.kaymera.com/industry-news-and-articles/what-happened-to-sky-ecc accessed 2 August 2025
[360] N1 Info (Balkan), 'Sky ECC data could be inadmissible in court' https://n1info.rs/english/news/balkan-insight-sky-ecc-data-could-be-inadmissible-in-court/ accessed 2 August 2025.
[361] N1 Info (Slovenia), 'Kavaski klan obtozena ne priznava krivde za umor' https://n1info.si/novice/crna-kronika/kavaski-klan-obtozena-ne-priznava-krivde-za-umor/ accessed 2 August 2025.

case has raised numerous privacy and fundamental rights concerns. Some lawyers argue that there was no individual suspicion (except for a few users), technical methods were not disclosed and access to the source and nature of the decrypted messages has been limited (i.e. it was not clear where the raw data exactly came from and if the raw data had been changed in any way after it had been collected). Some lawyers argue that this impairs the ability of defendants to challenge the authenticity and lawfulness of evidence. These and other circumstances raised questions about whether mass interception in the Sky ECC case violates points to violation of fair trial guarantees and the right to privacy (Articles 6 and 8 of the ECHR and the Charter).[362]

Additionally, the cross-border nature of the Sky ECC operation raised a distinct set of legal questions related to compliance of the cross-border transmission of evidence with fundamental rights under EU law and the ECHR.

Thousands of prosecutions across Europe remain ongoing, with several legal appeals filed concerning the admissibility of evidence and the right to a fair trial. Belgian and Dutch courts have largely upheld the legality of the interception.

In some cases, defendants have taken their claims to the constitutional and international courts, where certain proceedings are still pending. For instance, a defendant in Belgium, facing drug trafficking charges based almost exclusively on data obtained from mobile phones using the Sky ECC encrypted communication service, brought an action before the CJEU. He requested, first, that the Court declare the agreement establishing a Joint Investigation Team (the 'JIT Agreement') relating to Sky ECC inadmissible, and second, that it award him compensation for non-material damage under Article 268 TFEU. The defendant alleged that the damage resulted from acts committed by Eurojust, Europol, and several Member States. The *CJEU dismissed the action on the grounds that it was manifestly brought before a court lacking jurisdiction*.[363]

[362] Fair Trials, 'Why EncroChat and Sky ECC cases undermine the rule of law' (17 March 2025, updated 23 July 2025) https://www.fairtrials.org/articles/strategic-litigation/why-encrochat-and-sky-ecc-cases-undermine-the-rule-of-law/ accessed 2 August 2025.
[363] Case T-484/24 FF v Eurojust and Europol.

10 RECOMMENDATIONS FOR THE INCEPT PROJECT

Our data collection confirms that the EIO mechanism represents a significant achievement in cross-border evidence gathering for criminal investigations. Nevertheless, its practical application presents numerous questions and challenges, while also highlighting potential solutions and best practices. Eurojust rightly warns that '*the EIO Directive, and its underlying principle of mutual recognition, is not a magical formula*.'[364]

In this report, we have sought to address both the issues and challenges identified by Eurojust and the European Judicial Network (EJN) on the basis of Eurojust's casework, as well as those uncovered through our own research and observations. Based on these findings, we offer the following recommendations for the INCEPT project:

Recommendations on addressing challenges concerning the scope of the EIO Directive and the meaning and scope of 'interception of telecommunication'

Divergent interpretations of the scope of the EIO Directive, differences in the national transposition legislation, and the fact that the Directive does not define the terms 'telecommunications' or 'interception of telecommunications' creates legal ambiguity, particularly when interpreting Articles 30 and 31. This issue should be taken into account when designing the structure and content of national and international capacity-building events (T3.1-T3.5). The event's content should include contributions from experts who can address the interpretation and scope of the term 'interception of telecommunications'. This topic should be explored interactively, with active participation from attendees during both domestic and international events.

To support participants in clarifying the interpretation and scope of the EIO Directive – and specifically the concept of telecommunications interception – the EJN Secretariat's document '*Competent Authorities, Languages Accepted, Urgent Matters and Scope of the EIO Directive*' may serve as a helpful reference tool.

This lack of definition should also be considered when preparing both the INCEPT Methodology (T2.3) and the measures-related Questionnaire (T2.2). The questionnaire should seek input from participants (e.g., practitioners) on their understanding of the term 'interception of telecommunications'. It would be particularly valuable to compare the differences in responses across jurisdictions. The questionnaire should also explore any ambiguities or uncertainties practitioners encounter when interpreting or applying the concept.

Following the guidance from Eurojust and the EJN, practitioners should be asked how they distinguish between different types of interception, such as wiretapping and bugging – for example, whether they apply the same legal provisions to both in their daily practice. Additionally, they should be asked whether measures involving real-time interception of conversations, such as the transmission of stored traffic data related to a conversation, are treated under the specific provisions on telecommunications interception (Articles 30-31), or under the general regime of the EIO Directive.

Finally, the issues and challenges identified in this report in relation to the scope of the EIO Directive should also be considered during the development of the Manual on cross-border judicial cooperation in the use of telecommunications interception (T4.2).

Recommendations on addressing challenges related to the EIO's content and form

[364] See n 6, p. 51.

National and international capacity-building events should include expert guidance on addressing potential challenges when completing the EIO form (Annexes A, B, and C) in cases involving telecommunications interception, including issues related to language and translation (see Section 8.2).

When preparing the measures-related questionnaire for participants/practitioners, a set of questions should be developed to address the specific problems practitioners have encountered when filling out Annexes A, B, and C in the context of telecommunications interception. Participants should also be asked whether, in their daily practice, they attach the domestic judicial decision to the EIO, even though Article 5 of the EIO Directive on content and form does not establish such a legal requirement.

Additionally, the questionnaire should inquire whether participants experience any language or translation difficulties when dealing with EIOs.

The issues and challenges identified in this report regarding the EIO's content and form should also be addressed in the development of the Manual on cross-border judicial cooperation in the use of telecommunications interception.

Recommendations on addressing challenges related to issuing and transmitting the EIOs

The issues, challenges, and best practices related to the issuing and transmission of EIOs, as identified in Section 8.3 of this report, should be addressed during national and international capacity-building events through expert presentations and participant discussions or workshops.

The questionnaire should collect information from participants regarding their experiences with issuing and transmitting European Investigation Orders (EIOs). Participants should be asked, *inter alia*:

- Whether they have issued any EIOs for the interception of telecommunications, and if so, how frequently;
- Whether they consult the EJN document '*Competent Authorities, Languages Accepted, Urgent Matters and Scope of the EIO Directive'* when assessing whether an incoming EIO – whether for telecommunications interception or another investigative measure – has been issued or validated by a competent authority of another Member State;
- How they conduct the proportionality assessment (i.e. determining whether the requested interception of telecommunications or other investigative measure is necessary and proportionate in a given case) when acting as the issuing authority;
- Whether and how often they rely on the consultation mechanism under Article 6(1)(b) of the EIO Directive to verify whether the requested interception or other measure could have been ordered under similar conditions in a comparable domestic case;
- Whether and in what circumstances they issue a separate EIO for the interception of telecommunications when requesting multiple measures;
- Whether and how often they use channels other than direct communication with other Member States to ensure the rapid and secure transmission of EIOs and to guarantee their authenticity.

Finally, the challenges concerning the issuing and transmission of the EIO should also be incorporated into the Manual.

Recommendations on addressing challenges related to the EIO's recognition and execution

Project partners should encourage the relevant authorities in their countries to establish a centralised receiving authority – namely, a judicial body responsible for receiving European Investigation Orders (EIOs), recognising them where competent, and subsequently forwarding them to the appropriate executing authority. This step should be taken where such a structure has not yet been implemented.

The issues, challenges, and best practices related to the recognition and execution of EIOs, as identified in Section 8.4 of this report, should be addressed at both national and international capacity-building events. These should include expert presentations as well as discussions or workshops involving participants.

The questionnaire should gather information from participants regarding their experiences with the recognition and execution of European Investigation Orders (EIOs). Participants should be asked, *inter alia*:

- Whether and how often they consult the EJN Atlas to identify the competent executing authority and obtain relevant contact details (see Section 8.4.1);
- Whether and how often, when acting as the executing authority, they have made use of an alternative investigative measure under Article 10 of the EIO Directive;
- Whether, as the executing authority, they have ever invoked grounds for non-recognition or non-execution under Article 11 of the EIO Directive, and if so, which grounds;
- Whether they have ever issued or executed an EIO in an urgent case (see Section 8.4.6);
- In urgent cases, whether they have referred to the EJN document '*Competent Authorities, Languages Accepted, Urgent Matters and Scope of the EIO Directive'*;
- How they handle cases where a Joint Investigation Team (JIT) and an EIO are applied in parallel (see Section 8.4.7);
- Whether and how often they use the secure telecommunications systems of Eurojust and the EJN, or the European Commission's Secure Online Portal, for the exchange of electronic evidence;
- Whether and how often they rely on guidance from Eurojust and the EJN at various stages of the EIO life cycle, including drafting, transmission, recognition, execution, and follow-up.

Additionally, the issues related to the EIO's recognition and execution should be taken into account when preparing the Manual.

Recommendations on addressing challenges arising from the diversity of national legal frameworks

EIOs that initially appear straightforward can sometimes become more complex due to differences between national legal systems. Our analysis of the legal frameworks in the participating countries revealed significant variations in how telecommunications interception is regulated in their national law and addressed in the case law of regular and constitutional courts (see Sections 6-8 of this report). These differences often necessitate in-depth discussions before an agreement on recognition and execution can be reached between the issuing and executing Member States – sometimes with the support of Eurojust.

The differences between national legal systems identified in this report – and the related issues arising in the practical implementation of EIOs involving telecommunications interception – should be carefully considered by project partners and addressed throughout the execution of project tasks. In particular, these issues should be taken into account when designing the structure and content of national and international capacity-building events and should be appropriately reflected in the programs of those events.

When preparing the questionnaire for practitioners, a set of questions should be designed to address potential challenges in the use of EIOs for telecommunications interception arising from differences in national regulations. Respondents should be asked to indicate at which stage of the EIO lifecycle such challenges typically occur, and to identify which problems arise more frequently and which are less common.

Given that none of the four countries participating in the INCEPT project have an explicit legal basis for Trojan horse surveillance – and that such practices are permitted in all but Slovenia – project partners should ensure that all relevant aspects of issuing, validating, recognising, and executing EIOs for this highly intrusive measure are thoroughly explored during both national and international capacity-building workshops. Relevant issues concerning Trojan horse surveillance should also be addressed in the measures-related questionnaire.

The questionnaire for participants should also explore whether there have been cases in which evidence obtained via an EIO from another Member State led to discussions on fundamental rights due to differences between national legal systems regarding telecommunications interception. Notably, in the cases supported by Eurojust, no such discussions were reported.

Eurojust reports that in cases where telecommunications interception is carried out without the technical assistance of the notified Member State (Article 31 of the EIO Directive), Member States differ in how strictly they interpret their obligation to verify whether such interception would be lawful under their own domestic law. Some conduct only a formal review, while others assess substantive legality, which may lead to delays or even the blocking of the interception.

As this aspect of the EIO's application was not explored by the ZRS team during its review of national normative frameworks and case law, it should be addressed through data collection via the measures-related questionnaire, as well as through on-site discussions between speakers and participants at the capacity-building events.

Differences between national legal systems – and the related challenges in using EIOs for telecommunications interception – should also be appropriately considered in the preparation of the INCEPT Methodology and the Manual.

Recommendations on addressing challenges related to specific provisions on interception of telecommunications (Articles 30 and 31 of the EIO Directive)

Several recurring issues and challenges have emerged in Eurojust's casework concerning the implementation of specific provisions on the interception of telecommunications (see Section 8.5). These issues should be addressed and discussed by expert speakers and participants during the capacity-building events. Topics for discussion include:

- European Investigation Orders (EIOs) lacking key details,
- the use of intelligence service materials as evidence in criminal proceedings,
- authorisation periods for interception,

- the interception of communications involving non-suspects,
- the scope of interception,
- divergent interpretations of Article 31 concerning 'car bugging',
- the designation of competent authorities for receiving Annex C, and
- the insufficient content or clarity of Annex C.

It is particularly important that expert contributions during the capacity-building events address one of the central issues in implementing the provisions on telecommunications interception: the differences in national approaches to determining whether an interception would be authorised in a similar domestic case (as set out in Article 30 of the EIO Directive).

The above-mentioned issues and challenges should also be reflected in the measures-related Questionnaire and the Manual.

Recommendations on addressing ECtHR and CJEU case law and challenges related to the mass interception of encrypted telecommunications in the context of cross-border evidence gathering

The ECtHR and the CJEU have been called upon to address the risks to fundamental rights posed by telecommunications interception, including in the context of systems enabling bulk collection of electronic communications data. While the CJEU has primarily examined mass surveillance regimes through the lens of personal data protection and the right to privacy under the e-Privacy Directive and the General Data Protection Regulation (GDPR), it has also provided guidance in the field of judicial cooperation in criminal matters, including the application of the EIO.[365]

When secret surveillance measures were challenged before the ECtHR, the Court held that domestic law must be both accessible and foreseeable in its application, ensuring that such measures are used only when 'necessary in a democratic society.' This requires adequate and effective safeguards and guarantees against abuse. Regarding mass surveillance regimes, the ECtHR has emphasised the need to adapt and expand the safeguards established in its case law on targeted interception to address the specific challenges posed by bulk interception and the general retention and access to communications data.[366]

Considering the tension between law enforcement efforts to investigate serious transnational crime and the protection of privacy, data protection, and the right to a fair trial, both national and international capacity-building events should address the legal issues arising from ECtHR and CJEU jurisprudence on telecommunications interception, with particular attention to their rulings related to mass surveillance regimes (see Sections 7.1 and 7.2 and Section 9). Special attention should be given to the legal (and technical) dimensions of the high-profile EncroChat and Sky ECC cases.

The complex legal issues stemming from ECtHR and CJEU case law on telecommunications interception (particularly their rulings on mass surveillance) should also be taken into account when preparing the INCEPT Questionnaire, Methodology, and Manual.

[365] See n 9, p. 2.
[366] *Ibid*.

Project partners are encouraged to carefully review the report and highlight any additional issues, challenges, or examples of best and problematic practices related to the practical implementation of the EIO that should be further examined during their project activities. Additional practical challenges in the use of the EIO are also expected to be identified by participants during capacity-building events.

11 CONCLUSION

The main objective of this report is to present the results of secondary research and to identify existing knowledge in the field of cross-border judicial cooperation within the EU, specifically concerning the interception of telecommunications through the application of the European Investigation Order (EIO). The research focuses on the legal dimensions, while ethical and technical aspects of cross-border telecommunications interception fall outside the scope of this report. The field is exceptionally broad, complex, and often controversial, characterized by numerous legal issues and practical challenges.

The data analysis aim to support the development of the INCEPT Methodology (T2.3) and the measures-related Questionnaire (T2.2), guide the planning and delivery of capacity-building events (T3.1–T3.5), and facilitate the preparation of the Manual on cross-border judicial cooperation in telecommunications interception (T4.2). This process integrates insights from academic literature, related research projects, legal frameworks, and case law at both national and EU levels. We have done our utmost to ensure the relevance and quality of the survey, despite challenging circumstances during the process. One of the two lead researchers was simultaneously pursuing studies in the United States, while the other experienced a personal loss following the tragic death of a closest friend.

Despite these difficulties, we are confident that this report will contribute meaningfully to identifying existing gaps and potential best practices in response to the many challenges and complexities associated with the implementation of the EIO, and help project partners in their efforts to strengthen practitioners' knowledge, skills, and motivation for effective cross-border evidence exchange in criminal proceedings.

12 BIBLIOGRAPHY

Ambos K, *Treatise on International Criminal Law: Volume III: International Criminal Procedure* (2nd edn, OUP 2024)

Apollonio D, 'Criminal police drive with the handbrake on [Kriminalistična policija vozi z ročno zavoro]' (2024) 45 Pravna praksa

Bachmaier Winter L and Salimi F (eds), *Admissibility of Evidence in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair Trial Rights* (Hart Publishing 2024)

BayFHVR, 'D9.5 Dissemination materials and final report' (Deliverable D9.5, H2020 Project RAMSES, Grant No 700326, RAMSES Consortium 2019)

Bigo D and others, *Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law* (European Parliament 2013)

Blight J, 'ASIO telecommunications interception and data access powers' (2023) 48(4) Alternative Law Journal 288

Bronitt S and Stellios J, 'Regulating Telecommunications Interception and Access in the Twenty-first Century: Technological Evolution or Legal Revolution?' (2006) 24 Prometheus 413

Brunon-Ernst A, Gligorijevic J, Manderson D and Wrobel C (eds), *Law, Surveillance and the Humanities* (Edinburgh University Press 2025)

Capus N and Hohl Zuercher F, 'Revamping Anticorruption Criminal Law: The Making of (In-)Transparency. Negotiated Justice in Transnational Corruption – between Transparency and Confidentiality' (2024) 1–32

Celeste E and Formici G, 'Constitutionalizing Mass Surveillance in the EU: Civil Society Demands, Judicial Activism, and Legislative Inertia' (2024) 25 German Law Journal 427–46

Celeste E, 'The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios' (2019) 15 European Constitutional Law Review

CJEU Communications Directorate, Press Release (April 2024) https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-04/cp240077en.pdf accessed 2 August 2025

Climente A, 'D8.1 VICTORIA training methodologies and evaluation criteria definition' (VICTORIA Consortium 2017)

Climente A, 'D8.3 VICTORIA training content production and tools selection' (VICTORIA Consortium 2018)

Congram M, Bell P and Lauchs M, 'Communication Interception Technology' in Policing Transnational Organized Crime and Corruption: Exploring the Role of Communication Interception Technology (Palgrave Pivot 2013) https://doi.org/10.1057/9781137333797_6 accessed 4 August 2025

Council of Europe, 'CyberEast+' (Cybercrime Programme Office 2025) https://www.coe.int/en/web/cybercrime/cybereast-en accessed 31 July 2025

Council of Europe, Guide on Article 8 ECHR (28 February 2025) https://ks.echr.coe.int/documents/d/echr-ks/guide_art_8_eng accessed 2 August 2025

Dequeșnes A, Baudouin L, Debruyne C, Lanux T, Leleu S, Moritz M, Serap S and EXFILES Consortium, 'D2.1 Fundamental support study on encryption and fundamental rights' (Université Lille 2022)

Doronin V, 'Lawful interception–A market access barrier in the European Union?' (2023) 51 Computer Law & Security Review 105867

Drake WJ and Wilson EJ III (eds), *Governing Global Electronic Networks: International Perspectives on Policy and Power* (MIT Press 2008)

Dudka K, 'Private and Journalistic Wiretapping and Criminal Procedure' in I Nowikowski (ed), *Problems of Judicial Law Application. A Festschrift for Professor Edward Skrętowicz* (Lublin 2007).

Eicke T, 'Human Rights Protection of Non-Human Subjects from the Perspective of an ECtHR Judge' EJIL: Talk! (25 April 2025);

Erbežnik A, 'Impact of Digital Evidence Gathering on the Criminal Justice System: A Broader Perspective' in Vanessa Franssen and Stanisław Tosza (eds), *The Cambridge Handbook of Digital Evidence in Criminal Investigations* (Cambridge University Press 2025)

Erbežnik A, 'Sistem EU za čezmejno pridobivanje e-dokazov: Uredba (EU) 2023/1543 in Direktiva (EU) 2023/1544' (2024) 26(2) Odvetnik 44

Eurojust and European Judicial Network, 'Joint Note on the Practical Application of the European Investigation Order' (June 2019) https://www.eurojust.europa.eu/sites/default/files/assets/eurojust_ejn_joint_note_practical_application_european_investigation_order.pdf accessed 31 July 2025

Eurojust, 'European Investigation Order' (2025) https://www.eurojust.europa.eu/judicial-cooperation/instruments/european-investigation-order accessed 4 August 2025

Eurojust, 'Digital Criminal Justice Programme' (European Union Agency for Criminal Justice Cooperation 2025) https://www.eurojust.europa.eu/judicial-cooperation/instruments/digital-criminal-justice-programme accessed 31 July 2025

Eurojust, 'Report on Eurojust's casework in the field of the European Investigation Order' (November 2020) https://www.eurojust.europa.eu/sites/default/files/2020-11/2020-11_EIO-Casework-Report.pdf accessed 31 July 2025

European Commission, 'D8.1 Project Handbook' (TITANIUM Consortium) https://cordis.europa.eu/project/id/740558/results accessed 23 May 2025

European Commission, 'Roadmap: Effective and Lawful Access of Law Enforcement Authorities to Electronic Data' (24 June 2025) https://home-affairs.ec.europa.eu/news/commission-presents-roadmap-effective-and-lawful-access-data-law-enforcement-2025-06-24_en accessed 3 August 2025

European Commission, 'CREST Deliverable D1.4: Public final activity report: WP1 – Project management and coordination' (CORDIS 2019) https://cordis.europa.eu/project/id/833464/results accessed 2 August 2025

European Commission, 'D3.3 Best practices for EUROpean COORDination on investigative measures and evidence gathering' (15 January 2019) https://www3.ubu.es/eurocoord/wp-content/uploads/2019/06/D3.3-NATIONAL-REPORTS-ON-EIO_rev.pdf accessed 31 July 2025

European Commission, 'D8.2 training material and plan of training sessions for law enforcement agents' (Deliverable D8.2, H2020 Project RAMSES, Grant No 700326, RAMSES Consortium 2018)

European Commission, 'D8.8 Guide on privacy and ethics-by-design in law enforcement technology' (28 February 2023) https://inspectr-project.eu/resources/public/INSPECTr_Public_Deliverable_D8.8.pdf accessed 31 July 2025

European Commission, 'Deliverable D 6.3 SIMARGL Full solution release. Integration, Validation and Demonstration' (29 April 2022) https://cordis.europa.eu/project/id/833042/results accessed 31 July 2025

European Commission, 'European Informatics Data Exchange Framework for Courts and Evidence (EVIDENCE) – Project results' (CORDIS 2014) https://cordis.europa.eu/project/id/608185 accessed 31 July 2025

European Commission, 'Explanatory report on the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union' OJ C379/7

European Commission, 'Extract forensic information for LEAs from encrypted smartphones (EXFILES) – Project results' (CORDIS 2020) https://cordis.europa.eu/project/id/883156 accessed 31 July 2025

European Commission, 'Fighting Crime and Terrorism with an IoT-enabled Autonomous Platform (CREST) – Project results' (CORDIS 2019) https://cordis.europa.eu/project/id/833464 accessed 31 July 2025

European Commission, 'From mobile phones to court – A complete FORensic investigation chain targeting MOBILE devices (FORMOBILE) – Project results' (CORDIS 2019) https://cordis.europa.eu/project/id/832800 accessed 31 July 2025

European Commission, 'HEROES Deliverable D4.4 Manual for Early Identification of Potential Victims of Trafficking in Human Beings, Child Sexual Abuse and Child Sexual Exploitation' (CORDIS 2023) https://cordis.europa.eu/project/id/101021801/results accessed 2 August 2025

European Commission, 'Intelligence Network and Secure Platform for Evidence Correlation and Transfer (INSPECTr) – Project results' (CORDIS 2019) https://cordis.europa.eu/project/id/833276/results accessed 31 July 2025

European Commission, 'Internet Forensic platform for tracking the money flow of financially-motivated malware (RAMSES) – Project results' (CORDIS 2016) https://cordis.europa.eu/project/id/700326 accessed 31 July 2025

European Commission, 'Novel strategies to fight child sexual exploitation and human trafficking crimes (HEROES) – Project results' (CORDIS 2021) https://cordis.europa.eu/project/id/101021801 accessed 31 July 2025

European Commission, 'Project details: 723198' (EU Funding & Tenders Portal 2025) https://ec.europa.eu/info/funding-

tenders/opportunities/portal/screen/opportunities/projects-details/31070247/723198 accessed 31 July 2025

European Commission, 'RAMSES D8.2 training material and plan of training sessions for law enforcement agents' (CORDIS 2018)

European Commission, 'Revamping Anticorruption Criminal Law – Strategies and Consequences (RevACLaw) – Project results' (CORDIS 2020) https://cordis.europa.eu/project/id/864498 accessed 31 July 2025

European Commission, 'Secure Intelligent Methods for Advanced RecoGnition of malware and stegomalware (SIMARGL) – Project results' (CORDIS 2019) https://cordis.europa.eu/project/id/833042 accessed 31 July 2025

European Commission, 'TITANIUM Deliverable D3.5 User experience and forensics reporting guidelines' (CORDIS 2017) https://cordis.europa.eu/project/id/740558/results accessed 2 August 2025

European Commission, 'Tools for the Investigation of Transactions in Underground Markets (TITANIUM) – Project results' (CORDIS 2017) https://cordis.europa.eu/project/id/740558 accessed 31 July 2025

European Commission, 'TRACE Deliverable D10.11 – TRACE project's final conference' (CORDIS 2021) https://cordis.europa.eu/project/id/101022004/results accessed 2 August 2025

European Commission, 'TRACE Deliverable D7.4 – Assessment of the scope and efficacy of European cyber forensics and recommendations to improve capacities and policies on detecting illicit money flows' (CORDIS 2021) https://cordis.europa.eu/project/id/101022004/results accessed 2 August 2025

European Commission, 'Tracking illicit money flows (TRACE) – Project results' (CORDIS 2021) https://cordis.europa.eu/project/id/101022004 accessed 31 July 2025

European Commission, 'Video analysis for Investigation of Criminal and Terrorist Activities (VICTORIA) – Project results' (CORDIS 2017) https://cordis.europa.eu/project/id/740754 accessed 31 July 2025

European Court of Human Rights, 'Mass surveillance Factsheet' (June 2024) https://www.echr.coe.int/documents/d/echr/fs_mass_surveillance_eng accessed 1 August 2025

European Digital Rights (EDRi), 'CJEU Introduces New Criteria for Law Enforcement to Access Data' (24 October 2018) https://edri.org/our-work/cjeu-introduces-new-criteria-for-law-enforcement-to-access-to-data/ accessed 1 August 2025

European Informatics Data Exchange Framework for Courts and Evidence project http://www.evidenceproject.eu accessed 31 July 2025

European Informatics Data Exchange Framework for Courts and Evidence project, 'Deliverable D4.1' http://s.evidenceproject.eu/p/e/v/evidence-ga-608185-d4-1-413.pdf accessed 31 July 2025

European Judicial Network, 'Competent authorities, languages accepted, urgent matters and scope of the EIO Directive' (6 March 2020) https://www.ejn-

crimjust.europa.eu/ejnupload/DynamicPages/Competent%20authorities-languages%20accepted-scope-6%20March%202020.pdf accessed 4 August 2025

European Judicial Network, 'Joint Paper on Assistance in International Cooperation in Criminal Matters for Practitioners: What can we do for you?' https://www.eurojust.europa.eu/publication/joint-paper-ejn-ej-assistance-international-cooperation-criminal-matters-practitioners accessed 2 August 2025

European Judicial Network, 'Judicial Atlas' https://www.ejn-crimjust.europa.eu/Ejn2021/AtlasChooseCountry/EN accessed 2 August 2025

European Judicial Network,'Home' https://www.ejn-crimjust.europa.eu/ejn2021/Home/EN accessed 4 August 2025

European Law Institute, 'Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings' (8 May 2023) https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Proposal_for_a_Directive_on_Mutual_Admissibility_of_Evidence_and_Electronic_Evidence_in_Criminal_Proceedings_in_the_EU.pdf accessed 1 August 2025

Explanatory Report on the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union OJ C379/7 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2000_379_R_0007_01 accessed 4 August 2025.

Fadhil M, 'The urgency of the harmonization of interception regulation in the context of law enforcement' (2020) 3(2) Substantive Justice International Journal of Law 125

Fair Trials, 'Why EncroChat and Sky ECC cases undermine the rule of law' (17 March 2025, updated 23 July 2025) https://www.fairtrials.org/articles/strategic-litigation/why-encrochat-and-sky-ecc-cases-undermine-the-rule-of-law/ accessed 2 August 2025

Federal Constitutional Court (Germany), Press Release no 104/2025 (3 December 2024) https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2024/bvg24-104.html accessed 31 July 2025

Fennelly D, 'Data retention: the life, death and afterlife of a directive' (2019) 19 ERA Forum

Fitsanakis J, 'The Techniques of Communications Interception' in Redesigning Wiretapping (Springer, Cham 2020) https://doi.org/10.1007/978-3-030-39919-1_5 accessed 4 August 2025.

Flander B and Erbežnik A, 'Toolkit for Handling and Admissibility of Electronic Evidence: Empowering Legal Practitioners to Critically Review E-Evidence from the Procedural Rights Perspective' https://www.zrs-kp.si/wp-content/uploads/2024/07/INNOCENT_monografija_online_edition.pdf accessed 31 July 2025

Galli F, 'The interception of communication in France and Italy – what relevance for the development of English law?' (2016) 20(5) International Journal of Human Rights 666

Garamvölgyi B and others, 'Admissibility of Evidence in Criminal Proceedings in the EU' (2020) 3 Eucrim

Garamvölgyi B et al, 'Admissibility of Evidence in Criminal Proceedings in the EU' (2020) 3 Eucrim 201

Goodwin B, 'German court finds hacked EncroChat phone evidence inadmissible' ComputerWeekly.com https://www.computerweekly.com/news/366617630/German-court-finds-hacked-EncroChat-phone-evidence-inadmissible accessed 2 August 2025

Grabosky PN, Smith RG and Wright P, *Crime in the Digital Age* (Routledge 1998)

Hummert C and Pawlaszczyk D, *Mobile Forensics – The File Format Handbook: Common File Formats and File Systems Used in Mobile Devices* (Springer 2022)

Institute of Justice, *European Investigation Order* (2022)

INTERPOL, 'Digital forensics: Helping our member countries make best use of electronic evidence' (2024) https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics accessed 31 July 2025

INTERPOL, 'Project Leader' (2023) https://www.interpol.int/en/How-we-work/Innovation/Projects/Project-Leader accessed 31 July 2025

Jerman Blažič B and Klobučar T, 'Investigating crime in an interconnected society: Will the new and updated EU judicial environment remove the barriers to justice?' (2020) 34(1) International Review of Law, Computers & Technology 87

Juliussen B A, 'Monitoring, Governmental Data Access and the Invocation of Article 8 ECHR by Legal Persons' (2025) The International Journal of Human Rights, https://munin.uit.no/handle/10037/36407 accessed 2 August 2025

Kaymera, 'What happened to Sky ECC' https://blog.kaymera.com/industry-news-and-articles/what-happened-to-sky-ecc accessed 2 August 2025

Kisswani NM, 'Telecommunications (interception and access) and its Regulation in Arab Countries' (2010) 5(4) Journal of International Commercial Law and Technology 225

Klimczak J, Wzorek D and Zielińska E, *The European Investigation Order in Judicial and Prosecutorial Practice: Identified Challenges and Development Perspectives* (Institute of Justice Publishing, Warsaw 2022)

Kosta E and Kamara I (eds), *Data Retention in Europe and Beyond: Law and Policy in the Aftermath of an Invalidated Directive* (Oxford University Press 2025)

Kostenko O and Ghaziani VA, 'Admissibility of Illegally Obtained E-Evidence: A Critical Study of EU Law and the Precedents of the European Court of Human Rights' (2024) 2 European Journal of Privacy Law and Technologies

Loideain N, 'Not So Grand: The Big Brother Watch ECtHR Grand Chamber Judgment' (Information Law & Policy Centre Blog, 28 May 2021) https://infolawcentre.blogs.sas.ac.uk/2021/05/28/not-so-grand-the-big-brother-watch-ecthr-grand-chamber-judgment/ accessed 1 August 2025

Lynskey O, 'The Data Retention Directive Is Incompatible with the Rights to Privacy and Data Protection and Is Invalid in Its Entirety: Digital Rights Ireland' (2014) 51(6) Common Market Law Review

Milanović M, 'The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för Rättvisa' (EJIL: Talk!, 26 May

2021) https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/ accessed 1 August 2025

Ministry of Justice (Slovenia), 'Draft amendments to the Criminal Procedure Act' (EVA 2024-2030-0001) https://e-uprava.gov.si/.download/edemokracija/datotekaVsebina/657266?disposition=inline&lang=si accessed 2 August 2025

N1 Info (Balkan), 'Sky ECC data could be inadmissible in court' https://n1info.rs/english/news/balkan-insight-sky-ecc-data-could-be-inadmissible-in-court/ accessed 2 August 2025

N1 Info (Slovenia), 'Kavaski klan obtozena ne priznava krivde za umor' https://n1info.si/novice/crna-kronika/kavaski-klan-obtozena-ne-priznava-krivde-za-umor/ accessed 2 August 2025

Newell BC, Timan T and Koops B-J (eds), *Surveillance, Privacy and Public Space* (Routledge 2019)

Office of the Public Prosecutor (Czech Republic), 'Reports on Activities' https://verejnazaloba.cz/nsz/cinnost-nejvyssiho-statniho-zastupitelstvi/zpravy-o-cinnosti/ accessed 2 August 2025

Office of the Public Prosecutor (Czech Republic), 'Reports on Activities' https://verejnazaloba.cz/nsz/cinnost-nejvyssiho-statniho-zastupitelstvi/zpravy-o-cinnosti/ accessed 2 August 2025

Opitek P, 'Operational Control of End Devices' (*Prokuratura i Prawo* [*Prosecution and Law*] issue 4, 2023)

Paquet-Clouston M et al, 'European Investigation Order: Favor cooperationis…' (2023) 2 Yearbook of International Enforcement of Criminal Law and Procedure 371

Parlov I et al, 'Information Security and the Lawful Interception of Communications through Telecom Service Providers Infrastructure: Advanced Model System Architecture' (Hrčak Repository) https://hrcak.srce.hr/file/372916 accessed 4 August 2025.

Pesch PJ and Sillaber C, Computer Law Review International 18/6 (De Gruyter 2017) 166 ff

Podkowik J, Rybski R and Zubik M, 'Judicial Dialogue on Data Retention Laws: A Breakthrough for European Constitutional Courts?' (2021) 19 International Journal of Constitutional Law

Polčák R, Kyncl L and Svoboda D, *Interception of Electronic Communications in the Czech Republic and Slovakia* (Masaryk University 2016)

Registry of the European Court of Human Rights and European Union Agency for Fundamental Rights, 'Mass surveillance: ECtHR and CJEU Case-Law, Joint Factsheet' (February 2025), https://ks.echr.coe.int/documents/d/echr-ks/mass-surveillance accessed 2 August 2025

Rogalski M, *Procedural and Extraprocedural Wiretapping: Control and Recording of Conversations Based on the Code of Criminal Procedure and Special Acts* (Wolters Kluwer Polska, Warsaw 2019)

Rückert C, Journal of Cybersecurity 5/1 (2019) https://doi.org/10.2139/ssrn.2820634 accessed 1 August 2025

Sachoulidou A, 'The Court of Justice in Staatsanwaltschaft Berlin v MN (EncroChat): From cross-border, data-driven police investigations to evidence admissibility' (2024) 31(4) Maastricht Journal of European and Comparative Law 510

Šalamon NK, 'National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies – Slovenia' (Mirovni Inštitut 2014)

Šepec M, 'Masovni nadzor komunikacij: primer SKY-ECC' (2025) 44(15) Pravna praksa 6

Supreme Court of Slovenia, VSRS I Ips 15930/2017, 31 May 2018

Tropina T, 'Comparative analysis' in *Access to Telecommunication Data in Criminal Justice: A Comparative Legal Analysis* (Springer 2021) 11

Tudorica M and Bonnici JM, 'Legal framework for digital evidence following the implementation of the EIO Directive: Status quo, challenges and experiences in Member States' in MA Biasiotti and F Turchi (eds), *European Investigation Order* (vol 55, Springer 2023) 151

University College Dublin Centre for Cybersecurity and Cybercrime Investigation, 'FREETOOL' https://www.ucd.ie/cci/projects/freetool/ accessed 31 July 2025

University College Dublin Centre for Cybersecurity and Cybercrime Investigation, 'UNDERSERVED Cyber Threat Reporting Platform' https://www.ucd.ie/cci/projects/underserved/ accessed 31 July 2025

Vassilaki IE, 'Interception of telecommunications for criminal investigation – a comparative analysis' (1994) 10(5) Computer Law & Security Report 238

Ventre D and Guillot P, *Electronic Communication Interception Technologies and Issues of Power* (John Wiley & Sons 2023)

Verras P and Chapman P, 'European Investigation Order: Favor cooperationis, operational problems, solutions and technical practices via the report of the Eurojust' (2023) 2 Yearbook of International Enforcement of Criminal Law and Procedure 371

Wahl T, 'ECJ Ruled in EncroChat Case' (2024) eucrim https://eucrim.eu/news/ecj-ruled-in-encrochat-case/ accessed 3 August 2025

Watt E, 'Much Ado About Mass Surveillance - The ECtHR Grand Chamber "Opens the Gates of an Electronic Big Brother" in Europe in Big Brother Watch v UK' (2021) Strasbourg Observers

Zaharieva R, 'The European investigation order and the joint investigation team - which road to take: A practitioner's perspective' (2017) 18(3) ERA Forum 365

Zakrzewski R and Jarocha W, *Admissibility of Correspondence Control and Wiretapping* [*Kontrola Państwowa* (State Control)] (1997)

Zubik M et al, *European Constitutional Courts towards Data Retention Laws* (Springer 2021)

Cases

A L and E J v France (ECtHR, Apps nos 44715/20 and 47930/21, 24 September 2024)

Allan v United Kingdom (ECtHR, App no 48539/99, 5 November 2002)

Barbulescu v Romania (ECtHR, App no 61496/08, 5 September 2017)

Benedik v Slovenia App no 62357/14 (ECtHR, 24 April 2018)

Big Brother Watch and Others v United Kingdom [GC] (ECtHR, Apps nos 58170/13, 62322/14, 24960/15, 25 May 2021)

Breyer v Germany (ECtHR, App no 50001/12, 30 January 2020)

Bykov v Russia [GC] (ECtHR, App no 4378/02, 10 March 2009)

Case C-140/20 Garda Síochána (CJEU, 5 April 2022)

Case C-203/15 in C-698/15 Tele2 Sverige and Watson (CJEU, 21 December 2016) ECLI:EU:C:2016:970

Case C-207/16 Ministerio Fiscal (CJEU, 2 October 2018) ECLI:EU:C:2018:788

Case C-229/23 H. YA and Others II EU:C:2024:183

Case C-293/12 in C-594/12 Digital Rights Ireland and Kärntner Landesregierung et al (CJEU, 8 April 2014) ECLI:EU:C:2014:238.

Case C-324/17 Gavanozov I EU:C:2019:892

Case C-339/20 VD and SR (CJEU, 20 September 2022) EU:C:2022:703

Case C-349/21 H. YA and Others I EU:C:2023:265

Case C-350/21 Spetsializirana prokuratura (CJEU, 17 November 2022) EU:C:2022:896

Case C-670/22 *M.N. (EncroChat)* EU:C:2024:372

Case C-724/19 HP EU:C:2021:267

Case C-746/18 H.K. (Prokuratuur) (CJEU, 23 March 2021) ECLI:EU:C:2021:152

Case C-852/19 Gavanozov II EU:C:2021:894

Case T-484/24 FF v Eurojust and Europol

Cases C-511/18, C-512/18 in C-520/18 La Quadrature du Net et al. (CJEU, 6 October 2020) ECLI:EU:C:2020:791

Cases C-793/19 and C-794/19 SpaceNet and Telekom Deutschland (CJEU, 20 September 2022) EU:C:2022:702

Centrum för Rättvisa v Sweden [GC] (ECtHR, App no 35252/08, 25 May 2021)

Constitutional Court of Bulgaria, decision 1/10.02.1998 on constitutional case № 17/1997

Constitutional Court of Bulgaria, decision 10/15.11.2011 on constitutional case № 6/2011

Constitutional Court of Bulgaria, decision 10/28.09.2010 on constitutional case № 10/2010

Constitutional Court of Slovenia, decision U-I-144/19 (Part Three) Official Gazette 89/23

Constitutional Court of Slovenia, decision U-I-144/19 (Part Two) Official Gazette 2/23

Constitutional Court of Slovenia, decision U-I-144/19-52 Official Gazette 58/23

Constitutional Court of Slovenia, decision U-I-18/93 Official Gazette 25/96

Constitutional Court of Slovenia, decision U-I-25/95 Official Gazette 5/98

Constitutional Court of Slovenia, decision U-I-65/13 Official Gazette 109/12

Constitutional Court of Slovenia, decision U-I-8/04 Official Gazette 74/06

Constitutional Court of Slovenia, decision Up 2094/06 Official Gazette 20/08

Constitutional Court of Slovenia, decision Up 995/15 Official Gazette 56/18

Constitutional Court of Slovenia, decision Up-106/05-27 Official Gazette 81/08

Constitutional Court of Slovenia, decision Up-127/16 Official Gazette 15/22

Constitutional Court of Slovenia, decision Up-412/03-21 Official Gazette 117/2005

Constitutional Court of Slovenia, decision Up-62/98 Official Gazette 49/99

Constitutional Court of Slovenia, decision Up-899/16-18, Up 900/16-25, Up901/16-25 Official Gazette 43/22

Constitutional Tribunal (Poland), judgment of 12 December 2005, K 32/04

Data Protection Commissioner v Facebook (Schrems II) (C-311/18) EU:C:2020:559

Denisov v Ukraine [GC] (ECtHR, App no 76639/11, 25 September 2018)

Dragojević v Croatia (ECtHR, App no 68955/11, 15 January 2015)

Ekimdzhiev and Others v Bulgaria (ECtHR, App no 70078/12, 11 January 2022)

Halford v United Kingdom (ECtHR, App no 20605/92, 25 June 1997)

Higher Court in Ljubljana, judgment VI Kp 34126/2021

Higher Court Koper, decision Kp 229/2006

Huvig v France (ECtHR, App no 11105/84, 24 April 1990)

Iliya Stefanov v Bulgaria (ECtHR, App no 65755/01, 22 May 2008)

Iordachi and Others v Moldova (ECtHR, App no 25198/02, 10 February 2009)

Karabeyoglu v Turkey (ECtHR, App no 30083/10, 7 June 2016)

Katz v United States, 389 US 347 (1967)

Kennedy v United Kingdom (ECtHR, App no 26839/05, 18 May 2010)

Khan v United Kingdom (ECtHR, App no 35394/97, 12 May 2000)

Klass and Others v Germany (ECtHR, App no 5029/71, 6 September 1978)

Kopp v Switzerland (ECtHR, App no 23224/94, 25 March 1998)

L B v Hungary [GC] (ECtHR, App no 36345/16, 9 March 2023)

Liberty and Others v United Kingdom (ECtHR, App no 58243/00, 1 July 2008)

Naumenko v Latvia (ECtHR, App no 50805/14, 23 June 2022)

Niemetz v Germany (ECtHR, App no 13710/88, 16 December 1992)

P G and J H v United Kingdom (ECtHR, App no 44787/98, 25 September 2001)

Pietrzak and Bychawska-Siniarska and Others v Poland (ECtHR, Apps nos 72038/17 and 25237/18, 28 May 2024)

Podchasov v Russia (ECtHR, App no 33696/19, 13 February 2024)

Regional Court – Levski (Bulgaria), judgment 39/19.04.2012 on civil case № 280/2010

Roman Zakharov v Russia [GC] (ECtHR, App no 47143/06, 4 December 2015)

Schenk v Switzerland (ECtHR, App no 10862/84, 12 July 1988)

Schrems (Maximillian) v Data Protection Commissioner (C-362/14) EU:C:2015:650

Škoberne v Slovenia (ECtHR, App no 19920/15, 15 February 2024)

Supreme Administrative Court (Bulgaria), judgment 8687/27.06.2018 on administrative case № 10518/2017

Supreme Court of Cassation (Bulgaria), decision 1435/15.12.2012 on civil case № 815/2012

Supreme Court of Cassation (Bulgaria), interpretative decision 4/03.12.2014 on criminal division case № 4/2014

Supreme Court of Cassation (Bulgaria), judgment 10/07.10.2015 on criminal case № 1646/2014

Supreme Court of Cassation (Bulgaria), judgment 113/13.10.2020 on criminal case № 224/2019

Supreme Court of Cassation (Bulgaria), judgment 208/07.05.2025 on criminal case № 78/2025

Supreme Court of Cassation (Bulgaria), judgment 26/07.06.2016 on criminal case № 1626/2015

Supreme Court of Cassation (Bulgaria), judgment 273/08.08.2012 on criminal case № 796/2012

Supreme Court of Cassation (Bulgaria), judgment 44/10.04.2012 on criminal case № 3013/2011

Supreme Court of Cassation (Bulgaria), judgment 516/16.12.2009 on criminal case № 539/2009

Supreme Court of Cassation (Bulgaria), judgment № 83/19.06.2012 on criminal case № 3135/2011

Supreme Court of Slovenia, judgment I Ips 264/2005

Supreme Court of Slovenia, judgment I Ips 292/2004

Supreme Court of Slovenia, judgment I Ips 322/2008

Supreme Court of Slovenia, judgment I Ips 4259/2018

Supreme Court of Slovenia, judgment I Ips 44415/2010

Szabó and Vissy v Hungary (ECtHR, App no 37138/14, 12 January 2016)

Valenzuela Contreras v Spain (ECtHR, App no 27671/95, 30 July 1998)

Weber and Saravia v Germany (ECtHR, App no 54934/00, 29 June 2006)

Wieder and Guarnieri v United Kingdom (ECtHR, Apps nos 64371/16 and 64407/16, 12 September 2023)

Legislation and Legal Sources

Act amending the Criminal Procedure Act, CPA-P, (Slovenia), Official Gazette 53/24

Act No 104/2013 (Czech Republic) https://www.e-sbirka.cz/sb/2013/104/2025-01-01?f=104%2F2013&zalozka=text accessed 2 August 2025

Act No 127/2005 (Czech Republic) https://www.e-sbirka.cz/sb/2005/127/2025-01-01?f=127%2F2005&zalozka=text accessed 2 August 2025

Act No 141/1961 on Criminal Judicial Procedure (Czech Republic)

Act No 153/1994 (Czech Republic) https://www.e-sbirka.cz/sb/1994/153/2025-01-01?f=153%2F1994&zalozka=text accessed 2 August 2025

Act No 154/1994 (Czech Republic) https://www.e-sbirka.cz/sb/1994/154/2019-09-06?f=154%2F1994&zalozka=text accessed 2 August 2025

Act No 289/2005 (Czech Republic) https://www.e-sbirka.cz/sb/2005/289/2021-07-01?f=289%2F2005&zalozka=text accessed 2 August 2025

Act on Cooperation in Criminal Matters with Member States of the European Union (Slovenia), Official Gazette 48/13, 37/15, 22/18, 94/21

Charter of Fundamental Rights of the European Union OJ C364/1

Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC on the adequacy of the protection provided by the Safe Harbour privacy principles OJ L215/7

Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC on the adequacy of the protection provided by the EU-US Privacy Shield OJ L207/1

Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 on the adequate level of protection of personal data under the EU-US Data Privacy Framework OJ L231/118

Constitution of the Republic of Slovenia, Official Gazette of the Republic of Slovenia 33/91, 42/97, 66/00, 24/03, 69/04, 68/06, 47/13, 75/16, 92/21

Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union OJ C197/3

Council Framework Decision 2003/577/JHA on the execution in the European Union of orders freezing property or evidence OJ L196/45

Council Framework Decision 2008/978/JHA on the European evidence warrant OJ L350/72

Council Resolution on the lawful interception of telecommunications OJ C329/1

Criminal Procedure Act (*Zakon o kazenskem postopku*), Official Gazette of the Republic of Slovenia 176/21, 53/24

Criminal Procedure Code (Bulgaria), State Gazette of Bulgaria 86/2005

Czech Republic: Act No 141/1961 https://www.e-sbirka.cz/sb/1961/141/2025-02-11?f=141%2F1961&zalozka=text accessed 31 July 2025

Czech Republic: Act No 153/1994 https://www.e-sbirka.cz/sb/1994/153/2025-01-01?f=153%2F1994&zalozka=text accessed 31 July 2025

Czech Republic: Office of the Public Prosecutor https://verejnazaloba.cz/nsz/cinnost-nejvyssiho-statniho-zastupitelstvi/zpravy-o-cinnosti/ accessed 31 July 2025

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on privacy and electronic communications OJ L201/37

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC OJ L 105/54

Directive 2014/41/EU regarding the European Investigation Order in criminal matters OJ L130/1

Electronic Communications Act (Slovenia), Official Gazette of the Republic of Slovenia 130/22

Ministry of Justice (Slovenia), 'Draft amendments to the Criminal Procedure Act' (EVA 2024-2030-0001) https://e-uprava.gov.si/.download/edemokracija/datotekaVsebina/657266?disposition=inline&lang=si accessed 2 August 2025

Special Intelligence Means Act (Bulgaria), State Gazette of Bulgaria 79/1997

The Electronic Communications Act (*Zakon o elektronskih komunikacijsh* [ZEKom-2]), Official Gazette of the Republic of Slovenia 130/22

The Oversight of Intelligence and Security Services Act (*Zakon o parlamentarnem nadzoru obveščevalnih in varnostnih služb* [ZPNOVS]), Official Gazette of the Republic of Slovenia, no. 93/07 – officially consolidated text