SIRIUS CROSS-BORDER ACCESS TO ELECTRONIC EVIDENCE

EUROJUST

EUROPOL

EXTERNAL RESOURCES ON CROSS-BORDER ACCESS TO ELECTRONIC EVIDENCE

SIRIUS Annual Report

31/10/2024

The SIRIUS project has received funding from the European Commission's Service for Foreign Policy Instruments (FPI) under contribution agreement No PI/2020/417-500. This document was produced with the financial assistance of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union.

Contents

1. INTRODUCTION

The need for cross-border access to electronic evidence is imperative for a vast majority of criminal investigations and proceedings nowadays. In this context, a number of public and private entities and projects have been creating resources aimed at facilitating cross-border access to electronic evidence for different stakeholders involved in the process.

The SIRIUS Project, as a central reference point for knowledge sharing on cross-border access to electronic evidence in the European Union (EU), has developed this overview of the most relevant publicly available resources related to the topic of cross-border access to electronic evidence.

This list of resources, which have been created by entities other than the SIRIUS Project, is not exhaustive and will be periodically reviewed to include new and amend existing resources.

SIRIUS RESOURCES

Selected publications created by the SIRIUS Project, including more than 20 legal and policy reviews on topics of interest to cross-border access to electronic evidence, have been made publicly available via the SIRIUS subpage on Eurojust's website. The legal and policy reviews cover, among others, the following topics: the EU Electronic Evidence legislative package[1], the Council of Europe Convention on Cybercrime (also known as the Budapest Convention) and its Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (Second Additional Protocol), including specific articles thereof, the EU Digital Services Act, digital exchange platforms (e.g. eEDES, INTERPOL'S e-MLA initiative) and requesting mutual legal assistance (MLA) in criminal matters from specific jurisdictions (e.g. Ireland, Japan, Switzerland).

The full set of resources developed within the framework of the SIRIUS Project is accessible to law enforcement and judicial authorities from EU Member States and a number of third countries, as well as the European Public Prosecutor's Office, via a restricted SIRIUS platform hosted on the Europol Platform of Experts and the SIRIUS application available for Android and iOS.

2. EUROJUST-EUROPOL RESOURCES

A – JOINT EUROJUST-EUROPOL REPORTS ON COMMON CHALLENGES IN COMBATTING CYBERCRIME

The joint Eurojust and Europol report on Common Challenges in Combating Cybercrime, released in 2019, analyses five main challenges in combatting cybercrime from both a judicial and a law enforcement perspective, namely:

- Loss of data;
- Loss of location;
- Challenges associated with national legal frameworks;
- Obstacles to international cooperation; and
- Challenges of public-private partnerships.

The report also discusses ongoing activities and open issues for each of the five challenges identified.

[1] Consisting of Regulation (EU) 2023/1543 of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings and Directive (EU) 2023/1544 of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings.

The joint Eurojust and Europol report on Common Challenges in Combating Cybercrime, released in 2017, identifies and categorises the challenges in combatting cybercrime, predominantly from a judicial and law enforcement viewpoint, and is informed by operational and practical experiences. The report identifies six main areas:

- Loss of data;
- Loss of location;
- Challenges associated with national legal frameworks;
- Challenges of public private partnerships;
- Obstacles to international cooperation; and
- The rapidly developing threat landscape and the resulting expertise gap.

The document also looks at some of the practical implications of these challenges.

B – EUROJUST REPORTS

Eurojust's 9th issue of the Cybercrime Judicial Monitor (CJM), released in July 2024, covers legislative developments in the area of cybercrime, cyber-enabled crime and electronic evidence in 2023. The judicial analysis section presents brief summaries of court rulings from various EU Member States, including the ruling rendered by the Court of Justice of the European Union (CJEU) in April 2024 in case C-670/22 – *M.N. (EncroChat)*, clarifying the conditions for the transmission and use of evidence in criminal cases with a cross-border dimension. This issue of the CJM also covers the developments within the EU in the past year in relation to data retention.

Eurojust's 8th issue of the CJM, released in June 2023, covers legislative developments in the area of cybercrime, cyber-enabled crime and electronic evidence in 2022. It covers adopted legislation (e.g. the Digital Services Act) as well as ongoing procedures (e.g. the Artificial Intelligence Act). The judicial analysis section presents summaries of court rulings from various EU Member States and non-EU countries. In 2022, several European countries reported court rulings on the culpability of persons operating darknet marketplaces and the use of captured encrypted communication data. This issue of the CJM also covers data retention developments, including three preliminary rulings by the CJEU, providing additional guidance concerning the implementation of (supranational) data retention rules in European countries.

Previous editions of the CJM (released between 2016-2022) are also available in the Publications section on Eurojust's website.

C – REPORTS ON ENCRYPTION

The EU Innovation Hub for Internal Security's First Report on Encryption, released in 2024, contains an analysis of the topic of encryption from a legislative, technical and developmental viewpoint. It also touches upon certain specific judicial processes and court rulings about overcoming encryption in cases where it represents an obstacle for criminal investigations, especially in relation to evidence admissibility.

Eurojust and Europol's joint Third report of the observatory function on encryption, released in 2021, builds on previous reports and looks at the relevant technical and legislative developments regarding encryption, further elaborating on some of the topics covered by previous editions of the report.

Eurojust and Europol's joint Second report of the observatory function on encryption, released in 2020 contains an update on relevant statements or propositions made with respect to how law enforcement and prosecution can potentially cope with encryption and its related legal and technological challenges.

Eurojust and Europol's joint First report of the observatory function on encryption, released in 2019, provides an overview of the state of play with respect to encryption, including encryption challenges for law enforcement and prosecution.

3. UNODC RESOURCES

A- ELECTRONIC EVIDENCE HUB

The SHERLOC Electronic Evidence Hub is the United Nations Office on Drugs and Crime (UNODC)'s collection of legal resources and practical tools on electronic evidence.

I – PRACTICAL GUIDE FOR REQUESTING ELECTRONIC EVIDENCE ACROSS BORDERS

The Practical Guide for Requesting Electronic Evidence Across Borders provides practitioners (investigators, prosecutors, judicial authorities and national authorities responsible for MLA of the United Nations Member States) with best practice from experts in the field, legal procedures from over 20 states, and contact points to assist them to preserve and produce electronic evidence from service providers located in foreign jurisdictions.

II – MODEL MLA RESOURCES

The Model MLA Resources section includes:

- Standardized templates (Model MLAR for Stored Electronic Evidence; Model MLAR for Real-Time Collection of Traffic Data or Content Data);
- Checklists (MLA Request Checklist); and
- Model provisions on MLA involving electronic evidence (Model Law on Mutual Assistance in Criminal Matters (2007), as amended with provisions on electronic evidence and the use of special investigative techniques (2022); UNODC Model Treaty on MLA; The Commonwealth Model Law on Electronic Evidence).

III – DATA DISCLOSURE FRAMEWORK

The Data Disclosure Framework outlines practices developed by international service providers in responding to cross-border government requests for data. It aims to assist smaller technological companies and micro-platforms in understanding the basic concepts and technical knowledge for handling data and electronic evidence for law enforcement and criminal justice purposes in the cross-border context.

IV – MODEL FORMS

The Model forms on preservation and disclosure of electronic data, developed in cooperation with the SIRIUS Project, United Nations Counter-Terrorism Executive Directorate (UNCTED), European Union Agency for Law Enforcement Training (CEPOL) and the EuroMed Justice and EuroMed Police projects as well as representatives of the industry, are a set of three stand-alone model forms for requests for:

- Preservation of electronic data;
- Emergency disclosure of electronic data; and
- Voluntary disclosure of electronic data.

The model forms are conceived as a tool for ready use by national authorities seeking to send data request to service providers. Further guidance on how to use such resources and best practices to draft requests under voluntary cooperation are available on the restricted SIRIUS Platform.

The model forms are also available on the SIRIUS subpage on Eurojust's website.

V – ELECTRONIC EVIDENCE RESOURCES

The Electronic Evidence Resources section on SHERLOC provides easy access to materials concerning the collection of electronic evidence and its use in legal proceedings available on SHERLOC's Case Law Database, Database of Legislation and Bibliographic Database.

B – MLA WRITER TOOL

The Mutual Legal Assistance Request Writer Tool is an HTML-based stand-alone application, which aims to assist criminal justice practitioners in expeditiously drafting MLA requests. It provides them with guidance through each step of the drafting process and further helps them draft MLA requests by filling in all appropriate and relevant information.

4. UNCTED RESOURCES

UNCTED's Trends Report on The State of International Cooperation for Lawful Access to Digital Evidence: Research Perspectives aims to provide counter-terrorism policymakers, practitioners and experts with an overview of the current situation and challenges presented by the state of international cooperation for lawful access to digital evidence.

The report consists of three sections. The first section reflects on the current major legislative developments in the field. The second section considers notable trends – developments that are relevant to the coordinated global resolution of the cross-border data problem — and challenges for the future. The third section identifies several future policy goals aimed at addressing the challenges outlined in the second section.

5. COUNCIL OF EUROPE RESOURCES

A – EXPLANATORY REPORTS: BUDAPEST CONVENTION AND ITS SECOND ADDITIONAL PROTOCOL

I – EXPLANATORY REPORT TO THE BUDAPEST CONVENTION

The Explanatory Report to the Budapest Convention was adopted by the Committee of Ministers of the Council of Europe at its 109th Session (8 November 2001). It does not represent an authoritative interpretation of the Convention, but is intended to facilitate its application by providing a more detailed context and explanations of its provisions as understood by the drafters of the Budapest Convention.

II – EXPLANATORY REPORT TO THE SECOND ADDITIONAL PROTOCOL TO THE BUDAPEST CONVENTION

The Explanatory Report to the Second Additional Protocol was adopted by the Committee of Ministers of the Council of Europe at its 1417bis meeting (17 November 2021). It is intended to guide and assist Parties in the application of the Protocol (which will enter into force following its ratification by five Parties) and reflects the understanding of the drafters as to its operation.

B – GUIDANCE NOTES: BUDAPEST CONVENTION

Guidance Notes, which are adopted by the Cybercrime Convention Committee (T-CY), represent the common understanding of the Parties regarding the use of the Budapest Convention, also in light of legal, policy and technological developments.

For example, Guidance Note #3 on transborder access to data (Article 32) addresses the question of transborder access to data under Article 32 of the Budapest Convention, representing the common understanding of the Parties as to the scope and elements of the said Convention article.

Guidance Note #10 on production orders for subscriber information (Article 18 Budapest Convention) addresses the question of production orders for subscriber information under Article 18 of the Budapest Convention, representing the common understanding of the Parties as to the scope and elements of the said Convention article with respect to the production of subscriber information.

Guidance Note #13 on the scope of procedural powers and of international co-operation provisions of the Budapest Convention addresses the scope of domestic procedural powers and of the international co-operation provisions of the Convention on Cybercrime as well as of its Second Additional Protocol.

C – REPORTS: BUDAPEST CONVENTION

The T-CY Reports are a collection of documents issued within the framework of the work of the Cybercrime Convention Committee (T-CY), such as reports on the plenary meetings of the T-CY, reports prepared by its working groups and working papers prepared by the Secretariat to the T-CY.

For example, the background paper on Criminal justice access to data in the cloud: cooperation with "foreign" service providers, prepared by the T-CY Cloud Evidence Group, provides a snapshot of the policies and practices of some major service providers headquartered in the United States of America (US) regarding their "voluntary" disclosure of information to law enforcement authorities in foreign jurisdictions.

The final report on Criminal justice access to data in the cloud: Recommendations for consideration by the T-CY, prepared by the T-CY Cloud Evidence Group, summarises the challenges, issues and solutions identified by the said working group in relation to the matter at stake and comprises a set of recommendations for consideration and further action by the T-CY.

D – TEMPLATES: BUDAPEST CONVENTION

I – DATA PRESERVATION REQUEST (ARTICLES 29 AND 30 OF THE BUDAPEST CONVENTION)

The template for expedited preservation of data under Article 29 of the Budapest Convention and for expedited disclosure of preserved traffic data under Article 30 of the Convention was adopted by the T-CY to facilitate the preparation and acceptance of requests by Parties to the Convention. A number of bilingual templates are also available. The use of the template is optional.

II – MLA REQUEST FOR SUBSCRIBER INFORMATION (ARTICLE 31 OF THE BUDAPEST CONVENTION)

The template for MLA requests for the production of subscriber information under Article 31 of the Budapest Convention was adopted by the T-CY to facilitate the preparation and acceptance of requests by Parties to the Convention. A number of bilingual templates are also available. The use of the template is optional.

6. EUROMED JUSTICE RESOURCES

A – EUROMED DIGITAL EVIDENCE MANUAL

The EuroMed Digital Evidence Manual: Practical Guide for Requesting Electronic Evidence from Service Providers creates a common guideline for law enforcement and judicial authorities to address their requests for cross-border digital evidence. It assists practitioners with identifying and overcoming the legal and practical difficulties related to the gathering of electronic evidence and aims to ease the cooperation in the process.

The manual provides the following tools:

1. Mapping of the service providers relevant for the EuroMed region[2], including service providers' contacts and their focal points for cooperation with authorities, their rules for cooperation with law enforcement and judicial authorities and the cases in which they authorise direct requests from foreign law enforcement services.
2. Judicial request guidelines, describing the types of requests (judicial and non-judicial), the content and the procedure for each one of the requests, in order to be correctly processed by the US Department of Justice.
3. Standardization of procedures, proposing a "Simplified Uniform Request" for urgent requests, preservation requests and direct requests, together with some other templates to be used if the service provider does not have a dedicated template.
4. A practical approach to EU law and policies, describing the EU model for cross-border gathering of electronic evidence and the EU model for data protection.

B – EUROMED JUSTICE LEGAL AND GAPS ANALYSIS

The EuroMed Justice Legal and Gaps Analysis – Cybercrime analyses the context of cybercrime (legislative framework and international cooperation) in the South Partner Countries (Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Palestine[3] and Tunisia), identifies legislative gaps and, on that basis, makes recommendations to enhance their legal frameworks, investigation procedures and international cooperation.

The EuroMed Justice Legal and Gaps Analysis – Special Investigations Techniques, on the other hand, analyses the context of special investigation techniques (legislative framework and international cooperation) in the South Partner Countries.

7. US DEPARTMENT OF JUSTICE RESOURCES

A – A BRIEF EXPLANATION OF PROBABLE CAUSE FOR FOREIGN AUTHORITIES

A Brief Explanation of Probable Cause for Foreign Authorities sets out basic concepts surrounding the probable cause legal standard under US law. It intends to provide foreign authorities with sufficient understanding of the probable cause standard to assist them in formulating requests for assistance that depend on satisfying this legal standard.

B – FREQUENTLY ASKED QUESTIONS REGARDING LEGAL ASSISTANCE IN CRIMINAL MATTERS

Frequently Asked Questions Regarding Legal Assistance in Criminal Matters provides succinct answers to questions that foreign authorities may have on requesting MLA in criminal matters from the US.

C – CLOUD ACT RESOURCES

The US Department of Justice has created a page dedicated to CLOUD Act Resources which gathers in one place all official CLOUD Act-related materials, including Frequently Asked Questions on the CLOUD Act, any updates regarding CLOUD Act Agreements, as well as speeches and testimonies on CLOUD Act-related matters.

8. RESOURCES ON OBTAINING MLA FROM IRELAND

A – MLA RESOURCES

Mutual Legal Assistance in Criminal Matters: A Guide to Irish Law and Procedures was issued by the Department of Justice, Equality and Law Reform in its role as Ireland's Central Authority for MLA in criminal matters. It outlines Irish law in relation to international judicial cooperation in criminal matters with the intention to assist

[2] Algeria, Egypt, Israel, Jordan, Lebanon, Morocco, Palestine and Tunisia.
[3] This designation shall not be construed as recognition of a State of Palestine and is without prejudice to the individual positions of the Member States on this issue.

foreign authorities in making requests to Ireland for legal assistance for the purposes of criminal investigations or proceedings.

Additional information on the MLA process to Irish authorities, including its scope (i.e. what is not covered by the MLA process) and information for requesting authorities in relation to the kind of assistance they are seeking from the Central Authority, can be found on the dedicated MLA page of the Irish Department of Justice.

B – MLA REQUEST TEMPLATE

When the MLA request involves the production of specified evidential material for a criminal investigation (e.g. content data from an internet service provider), the requesting authorities may fill in a dedicated template for a Letter of Request designed to help them provide all the information and assurances required under Irish national legislation and by the courts when deciding on issuing production orders.

The information and assurances concerned can be provided either by completing the form and declaration of assurances contained in the template Letter of Request or by including the information and declaration in the requesting state's own Letter of Request.

9. RESOURCES ON OBTAINING MLA FROM SWITZERLAND

The website of the Swiss Federal Office of Justice, Switzerland's Central Authority for MLA in criminal matters, contains information on the MLA process towards Swiss authorities, including country-specific requirements and potential legal bases for requests (available in German, French and Italian).

Furthermore, a database of all Swiss localities and courts (searchable by postcode or name of the location) is available. This database contains information about each respective competent cantonal authority, its contact details, the legal basis on which judicial cooperation can be requested, as well as the official language(s) used.

10. RESOURCES ON OBTANING MLA FROM THE UNITED KINGDOM

A –MLA RESOURCES

The United Kingdom (UK) Home Office has made available a detailed guide for foreign competent authorities about obtaining evidence within the UK to assist in criminal investigations or proceedings.

The UK Home Office has also produced detailed MLA guidelines translated into Arabic, French, Italian, Polish, Portuguese, Spanish and Turkish for foreign authorities who want to make an MLA request to the UK.

B – STANDARD FORM FOR EU-UK MLA REQUESTS

As of 1 September 2023, all EU-UK MLA requests must be made using the standard form established under Article 635 of the EU-UK Trade and Cooperation Agreement. The form is available in all EU official languages on the website of the European Judicial Network (EJN).

C – ONLINE SUBMISSION FORM

As of 2 May 2024, the UK Central Authority has an online submission form (OSF) that allows EU Member States to send requests for MLA and freezing and confiscation to the UK instantly and securely, providing a more effective way of transmission. Countries outside the EU can utilise the OSF to send requests for MLA, freezing and confiscation and extradition. The OSF complements the standard form for EU-UK MLA requests mandated for use from 1 September 2023 and the standard forms for asset freezing and confiscation mandated by the EU-UK Trade and Cooperation Agreement.

11. RESOURCES ON OBTAINING MLA FROM JAPAN

The website of the Japanese Ministry of Justice contains information on the MLA process towards Japanese authorities, including guidance for sending MLA requests under both "non-treaty" and "with treaty" scenarios, as well as a checklist for drafting an MLA request to Japan. Additionally, it provides information on the legal acts and treaties governing the MLA process in criminal matters.

12. RESOURCES ON OBTAINING MLA FROM CANADA

The Department of Justice of the Canadian Government has issued the Requesting Mutual Legal Assistance from Canada: A Step-by Step Guide, which outlines Canadian law on international judicial cooperation in criminal matters. The guide is designed to assist foreign authorities in making requests to Canada for legal assistance in criminal investigations or proceedings.

Furthermore, the website of the Department of Justice of the Canadian Government contains information on the MLA process towards Canadian authorities, including details on the Mutual Legal Assistance in Criminal Matters Act, the Canada Evidence Act and information on bilateral and multilateral treaties that Canada is a Party to.

13. INTERNET & JURISDICTION POLICY NETWORK RESOURCES

A – TOOLKIT ON CROSS-BORDER ACCESS TO ELECTRONIC EVIDENCE

The Toolkit on Cross-Border Access to Electronic Evidence gathers resources to help different actors understand their roles in the process of cross-border access to electronic evidence. It offers practical tools for law enforcement and service providers to understand the different components of and thresholds for cross-border requests.

The toolkit is divided into two sections. The first section provides an overview of the structure and components of any cross-border regime for electronic evidence, serving as a guide for navigating its complexities. The second section adapts these components to voluntary disclosure, providing context and tools for states and providers to enhance the process of making (states) and handling (providers) such requests.

B – "WE NEED TO TALK ABOUT DATA" FRAMING REPORT

The report We Need to Talk About Data: Framing the Debate Around the Free Flow of Data and Data Sovereignty aims to untangle the two often polarising expressions related to data ("free flow" and "sovereignty"), providing a nuanced understanding of different perspectives and a reconciling approach to the debate around data.