Council of the European Union

Brussels, 9 December 2025
(OR. en)

15955/25

COPEN 375
EJN 13
JAI 1781

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	64th Plenary meeting of the European Judicial Network (EJN) (Warsaw, 7-9 May 2025) – Conclusions of Workshop 2: disclosure of e-evidence by service providers

Delegations will find attached the above-mentioned conclusions drafted by the EJN.

Workshop II

Disclosure of e-evidence by Service Providers Conclusions

I. Introduction

The second workshop of the 64th EJN Plenary Meeting focused on the challenges and opportunities in accessing and using electronic evidence (e-evidence) in criminal proceedings, with particular attention to cooperation with Internet Service Providers (ISPs). The workshop brought together EJN Contact Points to exchange experiences and best practices regarding the evolving legal and practical landscape on e-evidence, especially in cross-border contexts. The discussions highlighted the diversity of national approaches, the importance of cooperation mechanisms, the role of the EJN, and the role of emerging tools such as the e-evidence package, the Second Additional Protocol to the Budapest Convention, and platforms like KODEX and SIRIUS.

II. How to Request e-Evidence from Internet Service Providers (ISPs)

A core point of discussion focused on the means available for law enforcement and judicial authorities to obtain e-evidence from ISPs, particularly when those are located abroad. The approach taken depends significantly on the type of data sought—content data (e.g., the substance of communications) or non-content data (e.g., subscriber information, traffic data).

1. **Non-content data**:

Several participants noted that their national laws allow for direct requests to ISPs for non-content data, especially basic subscriber and traffic data. In practice, this may occur via:

- Direct cooperation under national law;
- Voluntary cooperation by the ISP, sometimes dependent on internal policies or Terms of Service;

- Orders or requests backed by enforceable national legislation and, in some jurisdictions, administrative or criminal sanctions for non-compliance.

However, theory and practice often diverge. While the legal framework may appear robust on paper, the practical enforcement of obligations on ISPs—especially foreign ones—remains uneven.

2. **Content data**:

Access to content data generally requires a formal judicial process and must follow instruments such as the European Investigation Order (EIO) or Mutual Legal Assistance (MLA) procedures. This remains true across most jurisdictions, particularly where no direct cooperation with ISPs is legally feasible.

When the ISP is in a third country:

- If the third country is a Party to the Budapest Convention, Articles 18 and 32 may provide a basis for direct access to certain types of data.
- If the country is not a Party to the Budapest Convention, the situation becomes more complex and often falls back on reciprocity arrangements, traditional MLA channels (such as the 1959 MLA Convention or UNTOC), or informal/voluntary cooperation frameworks.

Participants confirmed the continued importance of using MLA and EIO tools for the collection of content data, particularly in the absence of direct access mechanisms. However, delays—ranging from several months to over a year—remain a serious obstacle to efficient investigations.

III. Overview of ISPs Situated in Third Countries

Participants highlighted the fragmented landscape of ISPs, particularly those based in the United States and other non-EU jurisdictions. Access to data held by these providers is often governed by a patchwork of legal standards, voluntary cooperation agreements, and case-specific arrangements.

- ISPs located in third countries may require domestic legal process (e.g., a U.S. warrant), even for access to non-content data.
- Mutual understanding of procedural differences, including data protection standards and grounds for refusal, is key to navigating cooperation.

Participants also observed that some service providers appear to make strategic use of jurisdictional differences by relocating their operations to countries where judicial cooperation is particularly complex or limited. This practice, noted especially in relation to certain cryptocurrency exchange platforms, poses significant challenges for law enforcement and judicial authorities. While this issue may not be easily resolved through operational means, it was considered important to raise awareness of it at the political level, including in the context of the EU's engagement with such third countries.

This complexity has led to increased attention to international negotiations (e.g. EU-US negotiations and the Second Additional Protocol to the Budapest Convention), which aim to provide more clarity and operational efficiency.

IV. Data Retention

The discussion revealed widespread concern over the lack of harmonisation in data retention legislation across Member States.

Key issues include:

1. Existence or absence of national data retention regimes

Participants noted that some Member States have adopted data retention laws, while others have not. In jurisdictions without such legislation, service providers are generally only obliged to store data necessary for billing purposes, which severely limits the availability of information for investigative needs. This uneven playing field is one of the main reasons why the European Union is examining the possibility of establishing a common framework for data retention. This is considered a good option, since in certain cases the retention period can be as short as seven days—far too brief to be operationally useful, since many crimes are not detected within that timeframe.

2. Varying retention periods, from a few months to several years

Member States apply different rules regarding how long data must be kept. Some impose short-term obligations (e.g. 3–6 months), while others allow up to 2 years. This inconsistency complicates cross-border cooperation and undermines predictability in investigations.

3. Lack of uniformity in types of data required to be retained (e.g., traffic vs. content vs. subscriber data)

Not all Member States require the same categories of data to be retained. While most focus on subscriber and traffic data (metadata), others may include location data or exclude key types of internet metadata, which are essential for identifying users and reconstructing online activity.

4. Differences between retaining data and accessing retained data under legal authority

Even where data is retained, accessing it can be legally or procedurally difficult. Authorities often face restrictions based on proportionality, purpose limitation, or judicial authorisation, and access conditions vary greatly between Member States.

5. The need to distinguish between telecom data and internet data, with many jurisdictions treating these differently

Telecom data typically refers to metadata from traditional communications (e.g. phone calls, SMS), while internet data includes IP addresses, online session logs and metadata from social media or messaging platforms. The two are regulated differently, and internet data—often held by private ISPs—is subject to fewer or more fragmented obligations.

Participants broadly agreed on the importance of minimum EU standards, if not full harmonisation, to ensure a consistent legal and practical environment for data access. A common retention period—suggestions ranged from 6 to 12 months—was seen as a potential starting point for future discussion. Minimum standards could also help define the types of data to be retained and the procedural safeguards for access, fostering mutual trust and operational efficiency.

V. The Role of the EJN

The EJN was acknowledged as a valuable resource for practitioners and several proposals were made to enhance its support in the field of e-evidence:

1. Uploading on the EJN website national notifications concerning the implementation of the e-evidence package;

2. Providing country-specific information on data retention periods;

3. Clarifying national rules and exceptions related to privileged data;

4. Offering definitions for key data categories (e.g., content, traffic, subscriber data);

5. Making available Fiches Belges with summaries of national legislation and procedures;

6. Publishing Frequently Asked Questions and practical tips for effective information gathering;

7. Training activities aimed at improving the practical knowledge of legal practitioners working with electronic evidence;

8. Access to relevant case law, including national and European decisions that help interpret legal standards and practical approaches;

9. Sharing information and guidelines on data requests to third countries such as the USA and the UK, including procedures and possibilities for confiscation.

VI. KODEX

The KODEX project, designed to facilitate communication between law enforcement and ISPs through an automated and secure channel, was discussed in detail. The project is currently used by 229 entities worldwide.

Divergent views were expressed:

- Some Member States encourage its use, citing faster and more standardised exchanges with ISPs.
- Others voiced concerns about transparency, data protection, and lack of clarity regarding the platform's governance and oversight.

Participants noted the need for a better understanding of who manages KODEX, what safeguards are in place, and whether the tool complies with EU data protection standards. Despite these concerns, KODEX was seen as a potentially useful platform—provided these uncertainties are addressed.

VII. Final Conclusions

- The volume and complexity of cases involving electronic evidence will only increase. Legal tools must evolve accordingly.

- New EU instruments, particularly the e-evidence Regulation and Directive, provide a promising legal basis but require clear and practical implementation strategies.

- The EJN is well placed to act as a hub for practical guidance and coordination among judicial authorities.

- Legal certainty, data protection, and the effectiveness of cross-border tools must remain central to all developments in this field.

- Future EU policy should aim for interoperability between national systems and platforms like KODEX and SIRIUS, while ensuring transparency and safeguards.

- Ultimately, securing timely access to electronic evidence—under clear legal conditions and respecting fundamental rights—is essential to the functioning of the EU's Area of Freedom, Security and Justice.