Your Data, Their Jurisdiction: The EU's E-Evidence Revolution

15 SEPTEMBER 2026

Kinga Sztaba

Photo by George Prentzas on Unsplash

EU's E-Evidence Revolution

Starting from August 18, 2026, police forces of any EU state will be able to access your data stored on Signal, Meta, or WhatsApp directly from the service provider, provided that relevant judicial authorities pass on such. For law enforcement, it means a rapid and easy procedure; for fundamental liberties, it may pose certain obstacles, and most importantly- what does it signify for a case of an individual? A lot of criminal cases now, especially surrounding money laundering and cybercrimes in court, are built around information that goes beyond biometrics gathered from a weapon, CCTV material, or simple witness testimonies.

Thus, it is plausible that each day of waiting, the risk of evidence being tampered with or removed increases. Yet, until recently, obtaining this data often required months of mutual legal assistance procedures. Thanks to the Schengen Area, cyberspace and cybercrime recognize no national borders, as it functions on the transnational premise of digital evidence.

Yet, rules on admission of evidence and on criminal proceedings inevitably differ (Erbežnik, 2024, p. 51).

For years, prosecutors tracking cybercrime, drug syndicates, financial fraud, and terrorist networks across Europe ran into a valid dilemma of how location, possession, and custody of data play a role in their ownership. While criminal networks operated at the speed of fiber optics and encrypted communications, law enforcement authorities were forced to navigate through layers of diplomatic efforts, from broader Mutual Legal Assistance Treaties (MLATs) to EU-wide mechanisms available under the European Investigation Order (EIO). (Forlani, 2023, p. 3). Months of bureaucratic waiting meant that volatile digital data could have been deleted, encrypted, or altered long before a national judge could secure it (Tosza, 2020, pp. 168–169). To improve cross-border access to electronic evidence, the European Union adopted the e-evidence package in July 2023, comprising Regulation (EU) 2023/1543, with a specific date of implementation, and Directive being subject to rules on domestic transposition (EU) 2023/1544 (Forlani, 2023, pp. 2-4).

By creating a direct production-order mechanism in defined circumstances, the EU promised a needed acceleration, comparable with the one caused by the introduction of the European Arrest Warrant. This functional analogy is then visible as both instruments replaced an intermediary request-based model with the direct transmission of a judicial decision under the principle of mutual recognition, while structuring refusal around a limited set of legally defined grounds.

Yet, as the package transitions into full application across Member States, a fundamental question looms over Europe. Has cutting out intermediaries successfully solved the cross-border investigation dilemma, or has it simply traded one set of bureaucratic, yet fundamental, safeguards for exposing vulnerabilities?

Criminal Investigations Moved Faster Than the Law

The political momentum behind the E-evidence reform was fueled by the Commission's impact assessments. According to data cited by the European Commission, Electronic evidence is relevant in approximately 85 per cent of criminal investigations, and in almost two-thirds of those investigations, a request must be made to service providers based in another jurisdiction, meaning that approximately 55 per cent of all investigations involve a request for cross-border access to electronic evidence ('Commission Staff Working Document: Impact Assessment', SWD(2018) 118 final, 17 April 2018, p. 15). However, legal scholars have subjected these statistics by addressing the methodology of featuring such data; the underlying premise thus became ambiguous (Vazquez Maymir, 2020, pp. 1-15). For instance, academic analyses have noted that the Commission's impact assessments relied on fragmented datasets and biased samples, not reflecting the global trend, to support the case for reform (Vazquez

Maymir, 2020, pp. 2-9). Despite these debates performed by scholars, the overarching political consensus remained stable and concluded that traditional legal instruments were insufficient to address digital evidence.

Before the adoption of the E-evidence package, authorities relied primarily on the European Investigation Order established under Directive 2014/41/EU (Forlani, 2023, p. 3). While designed to foster judicial cooperation within the EU, these instruments suffered legal flaws established at a design level. In practice, there were territorial limits of investigative powers due to jurisdictional rules further influencing the control of electronic evidence (Tosza, 2024, pp. 239-242). In a nutshell, they did not account for extra-territorial illicit activities, like the manufacturing of CSAM that arose as a result of cooperation of users from different Member States. As a purely hypothetical and simplified illustration, a local drug trafficking ring in Berlin utilizing a server hosted in Dublin meant that German police had to ask Irish judicial authorities to request records from a U.S. cloud provider.

This model of cooperation generated two main issues. First, the process was relatively slow, frequently taking many months to yield results, which made it difficult against electronic data that could be erased or re-encrypted in seconds (Chavleski and Galev, 2019, pp. 1-2). Second, executing authorities in requested states frequently blocked or delayed requests based on domestic procedural hurdles or divergent interpretations of double criminality, resulting in absolute ground for refusal. Consequently, law enforcement faced severe impediments in prosecuting cross-border crime.

Five Years of Negotiations for Eight Hours of Waiting

The path to the e-evidence package included plenty of political and legislative tensions. Proposed by the European Commission in April 2018 (Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters', COM(2018) 225 final, 17 April 2018), the legislative initiative sparked five years of intense negotiations between the European Parliament, the Council of the European Union, and various stakeholders: from human rights NGOs to leading technology experts (Forlani, 2023, pp. 1-2). During the legislative process, significant friction arose over the appropriate balance between pace needed for the benefit of an investigation and fundamental rights, namely right to privacy. The European Parliament pushed for stronger judicial validation requirements prioritising direct involvement of judges, and broader grounds for refusal to protect individuals subject to foreign orders (and ultimately protecting state sovereignty by upkeeping state-made decisions in favor of foreign intervention) (Forlani, 2023, pp. 5-6).

Conversely, the Council advocated for direct, easier access and expediency. The final version, formally adopted on July 12, 2023, reflected a

victory for law enforcement who had signalled real needs for years (Regulation (EU) 2023/1543, 2023). Published as Regulation (EU) 2023/1543 and Directive (EU) 2023/1544, the package established a binding legal framework designed to facilitate investigations (Forlani, 2023, pp. 2-4). The choice of a regulation as the primary legislative act is also notable, with an objective of ensuring direct applicability across Member States from August 2023 onward, while leaving specific enforcement mechanisms and remedies to the exercise of State sovereignty. These include the domestic enforcement of non-compliant orders, the involvement of national courts in specified enforcement procedures, the imposition of penalties, the procedural framework for exercising remedies and any additional remedies available under national law. Separately, Directive (EU) 2023/1544 requires Member States to adopt national rules concerning designated establishments, legal representatives, central authorities and penalties (Regulation (EU) 2023/1543, 2023; Directive (EU) 2023/1544, 2023).

Two Instruments with One Single Goal

The E-evidence package currently consists of two instruments:

- Regulation (EU) 2023/1543: Establishes European Production Orders (EPOs) and European Preservation Orders (EPsOs). It enables competent judicial authorities to compel service providers offering services within the Union to preserve or produce electronic evidence directly, regardless of where the data or the provider is physically established (Tosza, 2024, p. 243).
- Directive (EU) 2023/1544: Imposes an obligation on service providers offering services in the EU to designate at least one establishment or legal representative in a Member State to receive, comply with, and execute these direct orders (Tosza, 2024, p. 243).

From Months to Days

First and foremost, service providers are bound by strict statutory- both ordinary and emergency- deadlines designed to mitigate data volatility. Standard production orders must be fulfilled within ten days of receipt, while emergency requests demand compliance within 6 to 8 hours (Albus, 2023, p. 7; Tosza, 2020, p. 174). In turn, preservation orders require providers to freeze specified data for up to 60 days, which is extendable upon request, to prevent tampering or deletion (Regulation (EU) 2023/1543, Articles 10 and 11).

To enforce compliance, the Regulation introduces financial sanctions applicable in the case of non-compliance. Providers failing to comply with an EPO or EPsO without valid justification face financial penalties reaching up to two percent of their total global annual turnover in the preceding financial year (Albus, 2023, p. 7). Working as an economic deterrent, possible penalties are expected to ensure that orders are fulfilled as a priority.

Furthermore, to balance investigatory powers against fundamental rights, the Regulation establishes a tiered categorization of data allowing for application of different procedural paths (Forlani, 2023, p. 9). It distinguishes between subscriber data and data requested solely for the purpose of identifying a user, on the one hand, and more sensitive traffic and content data, on the other. The less intrusive categories may be requested through a less demanding procedural route, whereas production orders for traffic and content data generally require review by a court or judge and may trigger notification of the enforcing authority. The latter authority may raise specified grounds for refusal, including certain fundamental-rights concerns, privileges and immunities, ne bis in idem and applicable double-criminality objections. This graduated approach is intended to connect the level of procedural scrutiny to the degree of interference with privacy, communications and data protection rights. It should nevertheless be treated as a potential safeguard rather than as proof that the Regulation achieves an effective balance in practice (Regulation (EU) 2023/1543, 2023).

Furthermore, communication and data transmission between authorities, legal representatives, and service providers are connected to decentralized and secure IT infrastructures such as e-CODEX, which shall operate as a significant safeguard for civil liberties (Tosza, 2024, p. 249; Ruiz, 2026, pp. 210–212). This infrastructure can mitigate technical risks such as interception, impersonation, unauthorised alteration and misdirection of orders or data. It does not, however, determine whether an order satisfies the requirements of legality, necessity and proportionality, nor does it guarantee timely notification, effective judicial remedies or consistent national protection of fundamental rights. E-CODEX should therefore be understood as a technical safeguard for the confidentiality and integrity of communications, rather than as a substantive safeguard for civil liberties (European Commission, 'E-evidence: Cross-border access to electronic evidence', 2026).

Cutting out the Middleman?

For tech giants and major service providers, dealing with European orders is potentially more predictable than navigating in twenty-seven distinct national legal regimes and conflicting administrative procedures. This standardisation may reduce legal uncertainty, although it does not eliminate national differences concerning enforcement, penalties, notification restrictions and additional remedies (Tosza, 2024, p. 237-260).

For investigating officers, the advantages are immediate and tangible (Forlani, 2023, p. 9). Rather than waiting for diplomatic clearance from a requested state, an investigating judge in one Member State can issue an order enforceable across the entire internal market, exemplifying the 21st-century version of the principle of mutual trust.

States Handing Over the Keys

Yet, speed and effectiveness may come at a price: reduced executing-state judicial scrutiny, weaker remedies, and jurisdictional uncertainty. Legal scholars have raised multiple objections regarding the framework's compatibility with fundamental rights and jurisdictional coherence (Albus, 2023, pp. 1-10). The most prominent systemic critique centers on what scholars call "privatised mutual recognition" (Albus, 2023, pp. 2-8). This term refers to the Regulation's direct channel between the issuing judicial authority and a private service provider, which may be required to receive and execute a European Production Order with limited involvement of authorities in the Member State where the provider is established (Regulation (EU) 2023/1543, 2023). Under EIO, an executing judicial authority acted as an independent filter that would check whether an incoming foreign request respects legal principles such as proportionality or the aforementioned double criminality. The EPO adopts a materially different model. Regulation (EU) 2023/1543 places responsibility for the legality, necessity and proportionality of the order primarily on the issuing authority, while the EPO is sent directly to the service provider.

An enforcing authority is normally notified only for orders seeking traffic data, other than data used solely to identify the user, or content data, and only where the order does not have sufficiently strong links to the issuing State. In those cases, the enforcing authority may assess the order and invoke the Regulation's limited grounds for refusal, including a manifest breach of fundamental rights and, subject to an offence-list exception, the absence of double criminality. For subscriber data and data requested solely to identify a user, no equivalent notification-based review is generally required.

The E-evidence framework relocates this second layer of judicial involvement. Consequently, the burden of executing criminal orders has been shifted from State organs to private corporate actors obligated to comply with orders (Albus, 2023, pp. 9-10). As different experts observe (Tosza, 2020, pp. 169-178), the European Production Order represents a radical leap in mutual recognition that lacks the necessary accompanying harmonization of procedural safeguards and remedies across Member States. Although the e-evidence package introduces important safeguards, it lacks fully harmonised accompanying rules on notification and secrecy, judicial review and legal aid, remedies in the enforcing State, challenges to European Preservation Orders, the protection of third parties and privileged data, and the admissibility and subsequent use of electronically obtained evidence. These matters remain partly dependent on national procedural law, creating uncertainty about where, when and by whom an affected person may challenge the measure and what consequences such a challenge will produce (Topalnakos, 2023, p.200).

When private entities are entrusted with compliance review, the public authority of judicial review by State organs is indirectly, yet virtually, delegated, which, according to some, signals a loss of control over endorsement performed by the executing state. This shift therefore blurs the boundaries between public criminal enforcement and private corporate compliance, raising fundamental questions about the accountability of multinational actors in criminal procedure (Erbežnik, 2024, pp. 47–48).

Your Data Travels Faster Than Your Rights

Individuals subjected to surveillance or data production in another Member State face significant obstacles in accessing effective judicial remedies (Tosza, 2020, pp. 176–178). Because the Production Order is transmitted directly from an issuing authority to a corporate entity, targets may remain entirely unaware that their private email correspondence, financial records, or cloud storage has been transferred across borders (Tosza, 2020, p. 178), producing certain doubts when it comes to legal certainty (Tosza, 2020, p. 178). While the Regulation delineates effective national remedies, the divergent legal standards and administrative procedures among Member States leave substantial gaps in judicial protection.

Furthermore, notification procedures are heavily restricted as in many cases, the issuing state is not required to notify the affected person or the state where the data is held until late in the proceedings, undermining the constitutional right to an effective defense (Albus, 2023, pp. 15–16). The lack of firm non-recognition grounds, which are restricted primarily to exceptional circumstances such as manifest violations of the Charter of Fundamental Rights, means that executing authorities in the provider's state have virtually no room to intervene on behalf of the individual (Albus, 2023, pp. 12-15). Consequently, individuals whose data is seized across borders may find themselves defenseless against disproportionate investigative measures originating in another Member State.

European Order v. American State of Mind

Apart from EU-based political tensions, the E-evidence package has a controversial position within different other instruments operating globally. A prominent unresolved challenge involves potential conflicts of law with third-country legislation, most notably the United States CLOUD Act (Tosza, 2024, pp. 245–246). When an EU-based subsidiary of a US-headquartered provider receives an EPO that conflicts with US blocking statutes, executive privilege, or foreign data privacy laws, the provider is trapped between conflicting legal obligations (Tosza, 2024, pp. 245–246). Although the Regulation contains provisions for review procedures when conflicting obligations arise, the actual effectiveness of these mechanisms remains entirely unproven.

Moreover, the operational success of the framework will depend heavily on parallel international agreements, such as a prospective EU-US agree-

ment on cross-border access to electronic evidence, as well as the technical implementation of e-CODEX across all participating Member States (Forlani, 2023, pp. 7-9). Discrepancies in national sanction regimes, where penalties for non-compliance are transposed unevenly across domestic legal orders, further threaten to ensure equal access to justice for individuals. (Tosza, 2024, pp. 245, 254–255).

Twenty- Seven Faces of One Regulation

As Member States work to transpose the E-Evidence Directive and apply a Regulation, domestic legal orders face severe tensions. National legislators must reconcile supranational production orders with existing data protection laws, notably the GDPR and their own constitutional safeguards. Discrepancies in how national courts interpret proportionality, standing for appeal, and compensation for unlawful data production may lead to uneven enforcement across the EU (Tosza, 2024, pp. 239, 245). Furthermore, legal practitioners across Europe are grappling with the practical realities of interfacing with decentralized IT networks and managing deadlines arising directly from the provisions (CCBE recommendations for Bars on the
implementation of the e-Evidence Regulation, 2024). These deadlines create practical difficulty because providers must identify, preserve, review, and securely transmit data across decentralised IT systems, often while handling substantial volumes of requests and navigating data stored across multiple jurisdictions

Is the e-Evidence Package Solving the Cross-Border Investigation Problem?

Returning to the central research question: Is the e-evidence package solving the cross-border investigation problem?

If success is measured by operational expediency, the E-Evidence package has the potential to improve cross-border access to electronic evidence by replacing some slower cooperation procedures with a direct production-order mechanism and shorter statutory deadlines (European Commission, 2018, SWD(2018) 118 final). It aligns legal instruments with the realities of digital information, rejecting simultaneously allegations that EU legislation seems to fail to act rapidly and that the legislative developments are always behind the technological progress.

However, if success requires balancing operational efficiency with judicial oversight and fundamental rights protection, the picture is more concerning for the right of privacy and the right of data protection. By embracing privatised mutual recognition and bypassing traditional judicial vetting in executing states, the framework renders legal remedies and fundamental rights potentially weakened. Ultimately, the cross-border investigation problem is no longer slowed down by diplomatic paperwork,

but it has found a more precarious aspect in endangering privacy-related individual rights and weakened judicial safeguards.