RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0216 • articolo sottoposto a peer review • pubblicato in anteprima il 29 apr. 2025

Rosanna Amato

Bridging borders, streamlining justice, balancing interests. The e-Evidence package journey: from a troubled origin story to an uncertain future

The increase in unlawful activities involving online platforms underscores the crucial role of digital evidence in judicial investigations. However, law enforcement and judicial authorities face significant challenges in accessing it. These challenges are particularly pronounced when digital evidence is stored on foreign infrastructures or held by service providers outside the investigation's jurisdiction, as both existing judicial cooperation mechanisms and informal agreements between authorities and service providers have proven inadequate. The EU's e-Evidence package marks a significant development aimed at addressing these challenges. However, despite its innovative nature, it is not without complications. This article explores the main features of the e-Evidence package, emphasising the components that support its functionality. After detailing the system and clarifying its complex elaboration process, the article assesses the potential of the current legal framework to meet its objectives. It focuses on operational aspects and identifies potential issues that may arise during implementation, which could impact its effectiveness.

e-Evidence – Judicial Cooperation – Cybercrime – European Union

Connettere le frontiere, snellire la giustizia, conciliare gli interessi. L'evoluzione del pacchetto e-Evidence: da un esordio problematico a un orizzonte incerto

L'aumento delle attività illecite condotte attraverso le piattaforme online sottolinea il ruolo cruciale delle prove digitali nelle indagini giudiziarie. Tuttavia, le autorità giudiziarie e di polizia incontrano difficoltà significative nell'accesso a tali prove, soprattutto quando queste sono conservate su infrastrutture estere o detenute da fornitori di servizi al di fuori della giurisdizione in cui viene svolta l'indagine. I meccanismi di cooperazione giudiziaria disponibili, così come gli accordi informali tra autorità e provider, si sono infatti rivelati carenti nel garantire un accesso tempestivo ed efficace alle prove digitali. Il pacchetto di norme dell'Unione europea in materia di *e-evidence* rappresenta un'importante evoluzione volta a colmare tali lacune. Tuttavia, nonostante il suo carattere innovativo, questo solleva numerose questioni di natura operativa e giuridica. Questo articolo esamina le caratteristiche principali del pacchetto *e-evidence*, soffermandosi sugli elementi che ne supportano il funzionamento sul piano operativo. Dopo aver delineato l'architettura del sistema e ricostruito il complesso iter che ha portato alla sua finalizzazione, l'analisi si concentra sul potenziale dell'attuale quadro normativo nel perseguire gli obiettivi prefissati. Particolare attenzione è riservata agli aspetti pratici e alle possibili criticità che potrebbero emergere nella fase di attuazione, con il rischio di comprometterne l'efficacia.

e-Evidence – Cooperazione giudiziaria – Crimine informatico – Unione europea

The Author is a researcher at the Institute of Legal Informatics and Judicial Systems of the National Research Council of Italy (office of Bologna)

1. Bridging the digital divide. Moving towards new solutions for EU e-Evidence gathering

Online platforms such as electronic communication services, social networks and marketplaces, together with their applications, increasingly contain information used in unlawful actions. For this reason, they often play a crucial role in judicial investigations, providing vital leads and evidence. The Europol 2023 SIRIUS Report highlights how data disclosed by service providers have been the sole investigative lead in crucial cases involving rape, human trafficking, fraud, phishing scams, aggravated sexual assault, and even terrorism. Without this data, these investigations would have been unsuccessful[1].

Today, a substantial part of criminal investigations depends on electronic evidence, which requires cross-border access to texts, images, emails or messages via apps. Between 2013 and 2016, requests for data from major tech companies such as Google, Twitter, Facebook, Microsoft, and Apple surged by 70%, as reported by EU Commission statistics, with over half of criminal investigations within the EU involving cross-border requests for electronic data. The Commission asserts that in 85% of these investigations, cross-border access to electronic evidence is necessary, with 65% of requests directed towards providers in different jurisdictions[2].

Law enforcement and judicial authorities notoriously struggle with access to such evidence. They often find themselves entangled in cumbersome legal procedures that hinder the swift acquisition of electronic evidence, as most available applicable legal instruments were created before the era of cloud computing and the widespread use of online services. This difficulty is compounded when evidence resides on private infrastructure located abroad or owned by service providers established outside the country where the investigation oc-

1. Europol 2024, pp. 19-20.
2. Commission Staff Working Document, Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings SWD(2018) 118, 17 April 2018. See also: Casino–Pina–López-Aguilar et al. 2022.

curs[3]. They can rely on various methods to obtain specific data from targeted individuals in criminal investigations, depending on the applicable law and other intervening factors, such as the location of data storage and public accessibility. In all such scenarios, however, acquiring usable evidence typically involves convoluted and lengthy processes. Existing mechanisms for cooperation between authorities have indeed proven inadequate, strained by the increasing number of cross-border cases and the rapid pace at which data can be altered or erased. Moreover, these arrangements are burdened by strict adherence to the principle of sovereignty, particularly in situations involving non-EU countries, where establishing a clear link between the crime and the requested data can be a significant obstacle.

Faced with these limitations, authorities have taken a proactive stance. They have formed partnerships with private service providers on a voluntary basis and thus created informal channels of cooperation running in "parallel" to legal assistance and mutual recognition instruments[4]. As of today, the volume of requests submitted to service providers under these parallel forms of cooperation is disproportionately higher than that of requests submitted through judicial cooperation[5]. Yet, the problem is that such a "voluntary approach" is not subject to any regulation, thereby leading to a complex landscape for competent authorities and service providers alike. On the one hand, the authorities are confronted with a maze of different obligations. These include legal requirements stemming from compliance with national laws, as well as those imposed by individual service providers who, in some cases, may not be willing to cooperate voluntarily at all, citing legal constraints, resource limitations or the lack of relevant policies. Further complicating matters is the admissibility of such data in court, which remains shrouded in uncertainty[6]. On the other hand, these ephemeral forms of collaboration also present a proving ground for service providers. Unclear requests by authorities, different (sometimes even conflicting) obligations, and a varied and ever-changing landscape of sanctions and procedural rules are significant challenges to their internal structure. These providers struggle to keep pace with the ever-evolving policies and regulations, hindering their ability to respond effectively and, in some cases, even deterring cooperation altogether.

In this context, facilitating the swift and legally sound gathering of electronic evidence for criminal investigations and prosecutions across the Union and beyond has become paramount. Notably, the last couple of years marked a turning point in this field, witnessing significant developments in the realm of international cooperation on electronic evidence. A major advancement came with the Second Additional Protocol to the Budapest Convention on Cybercrime, which introduces novel legal bases for direct cooperation to obtain domain name registration information and subscriber data for the purpose of investigations and prosecutions[7]. Moreover, international negotiations on the UN Convention on Cybercrime[8] have made significant progress, focusing on the inclusion of additional chapters which propose the criminalisation of specific cyber-dependent and cyber-enabled activities, providing a framework for international cooperation. Parallel to these developments, negotiations between the EU and the United States have resumed, with the aim to forge an international agreement to remove conflicts of law and facilitate access to electronic evidence[9]. 2023 also marked the enforcement of the EU Digital Services

3. SWD(2018) 118.
4. Sachoulidou 2024.
5. Europol 2024, p. 36 and p. 75.
6. *Ibidem*, p. 41 ss.
7. Council of Europe 2022. See also: Council of Europe 2023.
8. After three years of negotiations, the United Nations Convention against Cybercrime was adopted by the United Nations General Assembly on 24 December 2024 in New York by resolution 79/243. The Convention is the first comprehensive global treaty on this matter, providing States with a range of measures to prevent and combat cybercrime. It also aims to strengthen international cooperation in sharing electronic evidence for serious crimes.
9. Wahl 2023, pp 179-180.

Act (DSA) for very large online platforms[10], introducing standardised minimum requirements for orders to provide information under EU Member States' national laws[11].

Beyond these milestones, the most significant development in the field is the adoption of the new EU Electronic Evidence legislative package. This new system represents a legal revolution as it simplifies the process of obtaining electronic evidence in criminal cases by formalising direct requests to private providers of communication, Internet infrastructure service and data storage based in another Member State, generally avoiding the need to involve authorities in the service provider's home country. Although the legislation will not fully enter into force until mid-2026, its approval provides a clear roadmap for EU Member States and service providers to adapt their procedures and ultimately usher in a future of greater legal certainty and efficacy in obtaining electronic evidence across borders.

The EU e-Evidence initiative is composed of two legislative components:

– a Regulation[12] designed to streamline and expedite the process of securing and acquiring electronic evidence that service providers in a different jurisdiction store or possess. It allows national authorities to send an order to preserve (European Preservation Oder) or produce (European Production Order) data directly to the service provider's appointed representative, who is then required to comply by directly delivering the data to the requesting authority.
– a complementing Directive[13] that mandates service providers operating within the EU appoint a legal representative in at least one Member State, thus ensuring that orders and decisions issued under the above Regulation reach the proper recipients.

Designed to work within the existing judicial cooperation framework, these mechanisms do not replace previous instruments but aim to supplement them, particularly the European Investigation Order (EIO). Overall, central to this initiative are (i) simplifying the processes of acquiring and preserving electronic evidence within the EU, (ii) standardising the obligations of service providers, (iii) improving criminal investigations and prosecutions, and (iv) strengthening the protection of individual rights and fundamental freedoms.

Against this backdrop, this article aims to assess the potential of the current legal framework to achieve its objectives. The investigation adopts an operational lens, hypothesising potential challenges that may arise during the implementation phase. To this end, the paper examines the key features of the e-Evidence package, with a particular focus on the core elements underpinning its functionality: the decentralised IT system and the obligations set forth by Directive 2023/1544. Additionally, the article delves into the complex negotiations that culminated in the adoption of the package, with the primary goal of clarifying the motivations and objectives that the European legislator seeks to achieve through this new system. Finally, the analysis explores the Directive's potential benefits alongside its challenges, focusing on organisational and technical capacity, operational and technical tools, and the interplay with other legal frameworks.

This work is, thus, structured into three parts. First, an overview of the new electronic evidence collection system will be provided. This section (paragraph 2) explains the main features and operational mechanisms of the cooperation framework established by the Regulation, including a focus on the decentralised IT system for the exchange of relevant communications and documentation. Then, the Directive's obligations for participating countries, national authorities, and private stakeholders will be detailed. The second section (par-

10. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), Art. 10.
11. European Commission 2023.
12. The Regulation lays down the rules and safeguards for national authorities to order service providers located in another Member State to preserve and produce e-evidence for the purpose of carrying out criminal proceedings.
13. Directive (EU) 2023/1544 of the European Parliament and of the Council 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.

agraphs 4 and 5) delves into the negotiation and legislative process that led to the finalisation of the e-Evidence package. It highlights the various positions at stake, illustrating how this innovative system navigates the delicate balance between potentially conflicting priorities. This "glimpse into the past" aims to show how the differing views of States, institutional actors, and stakeholders have influenced the achieved outcomes. The final section (paragraph 6), on the other hand, aims to take a "peek into the future" so as to envisage potential challenges and operational issues that might emerge during the implementation phase.

2. The new EU system of e-evidence gathering: how does it work in a nutshell

The new e-Evidence package creates a framework for Member States that outlines how to handle data access requests from authorities within other EU jurisdictions during criminal investigations. Specifically, the Regulation details the type of requests authorities can present to private organisations applicable across the Union when they need to access specific user data for the purpose of obtaining electronic evidence[14] in criminal proceedings: the European Production Order and the European Preservation Order.

The European Production Order is an instrument that allows a judicial authority in one Member State to request and obtain preserved electronic evidence (such as e-mails, texts or app messages, together with information to identify a perpetrator as a first step) within a considerable tight timeframe. On the other hand, the European Preservation Order is a tool that allows a Member State's authority to request that specific data be retained and preserved for a subsequent data production request, thus preventing the deletion or altering of this data. Both are decisions issued or validated by the judicial authority of a requesting Member State.

What makes such a new regime groundbreaking is the mechanism upon which it rests: a direct dialogue between national authorities and private parties, which streamlines the process and aims for higher efficacy. Mirroring other EU judicial cooperation instruments built on the mutual recognition principle, European production and preservation orders utilise standardised multi-lingual templates: the European Production Order Certificate (EPOC) and the European Preservation Order Certificate (EPOC-PR)[15]. In addition, they follow standardised procedures, within which pre-defined timeframes and conditions must be met. These critical elements are designed to guide all participants in drafting, transmitting, and executing requests, thereby minimising ambiguities and fostering a level playing field between the requesting and requested parties across Europe.

The authority empowered to issue a European Production Order or Preservation Order hinges on two factors: the specific instrument chosen and the data category requested. This distinction reflects the varying scope of each measure and the differing impact on fundamental rights associated with different types of data.

Notably, when it comes to EPOC-PR, the issuing authority can be a judge, a court, an investigating magistrate or a prosecutor. The same applies to the EPOC, but only if an order must be forwarded to acquire subscriber data and certain traffic data used solely for user identification, such as IP addresses and access codes. A stricter process applies when EPOC involves traffic or content information, which is more intrusive. In these cases, only a judge, court, or investigating magistrate can issue a production order. The Regulation also permits the issuance of EPOC and EPOC-PR by other competent authorities designated by the issuing state, acting as investigating authorities in criminal proceedings and holding the power to gather evidence under national law. However, these orders require validation by a judicial authority to ensure compliance with the Regulation provisions and potentially applicable national law. This prior validation can be waived only in specific emergencies, and even

14. The Regulation defines the term "electronic evidence" as subscriber data, traffic data or content data stored by or on behalf of a service provider in an electronic form (Art. 3(8)), i.e., emails, text messages or content from messaging apps, audio-visual content, or information about a user's online account. These categories are coherent with the EU *acquis*, the EU Court of Justice jurisprudence and other international instruments (e.g., the Convention on Cybercrime of the Council of Europe, Budapest Convention).

15. Regulation (EU) 1543/2023, Art. 9.

then, the issuing authority must obtain ex-post validation within 48 hours.

Once issued, an EPOC or EPOC-PR can be transmitted directly to the service provider operating in one or more Member States, which becomes responsible for executing the request, either by preserving existing data (for EPOC-PR) or producing it (for EPOC). Upon receipt of a European Preservation Order, the service provider is obliged to preserve the requested data for a period of 60 days, after which the preservation duty ceases. However, there are two circumstances that can extend this period: the issuing authority confirms that an EPOC has already been issued or is forthcoming. In these cases, the service provider must retain the data for as long as it takes to produce them.

As far as the EPOC is concerned, it requires a very fast turnaround, as service providers must make the requested data available within 10 days, with an expedited timeframe of 8 hours in emergency situations. Only if the transmitted order targets traffic or content data a suspension period is foreseen[16]. In consideration of the sensitive nature of these types of data, the issuing authority, while forwarding the request to the service provider, has to notify the authority of the requested State (executing authority)[17] and simultaneously forward the standard certificate to it. This will allow the executing authority to assess whether the (few) grounds for refusal provided for in Regulation[18] apply to the case at hand. Such grounds for refusal may be raised within a period of 10 days (or 96 hours in emergency cases). Otherwise, they are deemed not to have been raised, and the strict time limits imposed on service providers remain in effect.

Consultation procedures are foreseen by the Regulation to smooth the dialogue between issuing and enforcing authority. Notably, the issuing authority about to emit an EPOC to obtain traffic or content data may seek prior clarification from the competent authorities of the executing State – directly or through Eurojust or the European Judicial Network – as to whether such data are protected by immunities, privileges granted by the law of the executing State, or other reasons expressly indicated in the Regulation, which may give rise to a legitimate refusal to execute the request[19]. Likewise, before deciding not to recognise or execute an EPOC or EPOC-PR, the executing authority is called upon to consult the issuing authority by any appropriate means for further information, which must be provided within five working days[20].

At the end of this process, should the service provider fail to provide or preserve the evidence requested, a common pecuniary penalty regime applies[21]. The Regulation does not provide for any specifics on this matter but merely stipulates that such financial penalties must be effective, proportionate and dissuasive. However, it requires Member States to ensure that financial penalties of up to 2% of the service provider's total annual worldwide turnover in the preceding business year may be imposed.

2.1. Digitalising cross-border dialogue for the purpose of gathering e-evidence

The Regulation mandates that document transmission and communications for the cooperation mechanism under discussion be conducted exclusively through digital means, with the exception of a few circumscribed situations. This emphasis on digitalisation is notoriously not an isolated effort but rather aligns with a broader strategic and regulatory trend aimed at modernising judicial cooperation by leveraging the potential of available IT tools for the exchange of communications and transmission of documents[22]. Digitalisation is, indeed, increasingly recognised as essential for enhancing the effectiveness and resilience of cross-border judicial cooperation in the EU, which has historically been hampered by reliance on pa-

16. *Ivi*, Art. 10 (2) (4).
17. *Ivi*, Art. 8 (1).
18. *Ivi*, Art. 12.
19. *Ivi*, Art. 5 (10).
20. *Ivi*, Art. 17 (7).
21. *Ivi*, Art. 16 (10).
22. See: "Proposal for a Regulation on the digitalisation of judicial cooperation and access to justice in cross-border civil, commercial and criminal matters, and amending certain acts in the field of judicial cooperation", Brus-

per-based communication[23]. The rapid expansion of IT applications among individuals, businesses, and institutions – intensified by the urgency of the COVID-19 pandemic – has further accelerated the shift towards fully digital processes, highlighting the necessity of a unified framework where technology is not merely an option but the preferred method for efficient cross-border cooperation[24].

The e-Evidence package embodies this approach by introducing procedures that are, by design, tailored to the digital realm. Barring a few occurrences, it requires all exchanges between competent authorities and private parties to be conducted through a secure and reliable decentralised IT system. This system integrates the IT infrastructures of Member States and Union agencies, utilising interoperable access points for interconnection. Service providers must use this decentralised system via their national IT structures to receive and respond to EPOCs and EPOC-PRs, ensuring swift, direct, and secure cross-border communication while reducing costs and delays for involved parties.

Although the Regulation body does not specify which decentralised system should be used to perform such an exchange, Recital 83 indicates that the access points should be based on e-CODEX (e-Justice Communication via Online Data Exchange)[25]. The e-CODEX system is designed to facilitate cross-border electronic data exchange in civil and criminal judicial cooperation – including text, audio, video, and metadata – thereby enhancing efficacy and access to justice. The system comprises two main components: a gateway for secure message exchange and a connector that links the national gateway to the national application, verifies electronic signatures, ensures message and attachment integrity, supports semantic interoperability, and provides proof of delivery[26].

Such mention in the Regulation's preamble is, after all, not surprising. The e-CODEX system has become crucial to the EU's digital justice strategies. Initiated in 2010 by a consortium of Member States' Ministries of Justice with EU financial backing, the system has continued to evolve and strengthen. Given its pivotal role in cross-border exchanges, it is now established through the EU legal framework, which includes operational and developmental rules, as well as measures to protect fundamental rights in line with the EU Charter of Fundamental Rights. Along with this, the management of e-CODEX will be entrusted to the European Union Agency for the operational management of large-scale IT systems in the area of freedom, security, and justice (eu-LISA). This will ensure the system's long-term sustainability and governance while upholding judicial independence. In conjunction with the e-EDES components developed by the EU Commission[27], this system has already shown its practical benefits and is on track to become the main digital solution for secure electronic data transmission in cross-border civil and criminal cases, aiding both in crime fighting and victim involvement. Compared to traditional communication methods, it offers superior standards in terms of speed, secure transmission, data protection, and confidentiality.

2.2. Directive (EU) 2023/1544 to designate establishments or appoint legal representatives for the purpose of gathering e-evidence

The concise description of the system established by Regulation 2023/1543 makes it readily apparent that in order to make the information exchange mechanism between authorities and providers effective, clarity on the players involved and their

sels COM(2021) 759, 1 December 2021; Regulation (EU) 2022/850 of 30 May 2022 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system), and amending Regulation (EU) 2018/1726; and, two recast regulations from November 2020, that is, the Regulation 2020/1784 of 25 November 2020 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters (service of documents) and the Service of Documents Regulation.

23. Ontanu 2022.

24. *Ibidem*.

25. Regulation (EU) 2022/850.

26. Velicogna 2014 and Velicogna 2018; Velicogna–Steigenga–Taal–Schmidt 2020.

27. Ben Miloud–Nicolau 2023.

respective responsibilities is imperative. In this context, Directive 2023/1544 is at the heart of the new system of cooperation introduced with the e-Evidence package[28].

The Directive aims to boost legal certainty and effectiveness as it seeks to deter Member States from autonomously addressing legal gaps related to acquiring e-evidence in criminal cases, thus leading to a patchwork of national requirements. Such a scenario has, indeed, not only proved to hinder criminal prosecutions but also to obstruct the seamless provision of services across the internal market. This new piece of legislation's primary aim is to streamline the process of receiving, complying with, and enforcing decisions in a cross-border setting, thereby facilitating the gathering of e-evidence across the EU without overstepping the existing powers of the requested Member State's authorities. Its key element is the obligation for service providers offering services in the Union to designate establishments or appoint legal representatives to handle decisions and orders from Member States' authorities regarding gathering evidence in criminal proceedings. This obligation applies to both EU-established service providers and those outside the EU offering services within it (this is the case for some large companies located in the United States). The sole exemption is for service providers established and operating exclusively within one Member State. Guidelines are laid down concerning where these representatives or establishments should be based, the responsibilities they should hold, and the resources they must rely on to fulfil their obligations, together with a timeline by which service providers must comply with these requirements[29].

As a matter of principle, service providers are free to decide about the number of designated establishments or legal representatives they appoint and in which Member States. Yet, the Directive does not fail to specify that both designated establishment and legal representatives be located in one or more Member States where the service provider operates or is established[30]. Aiming to prevent small and medium-sized enterprises from being disproportionately affected, the Directive allows a single establishment or appointed legal representative to serve several service providers as long as data protection safeguards are maintained[31].

These core provisions are then complemented by ancillary measures that aim to ensure the effectiveness of the stated obligation. On the one hand, Member States are required to appoint central authorities to ensure consistent and proportionate implementation of the Directive[32]. Service providers are then obliged to formally communicate to these central authorities the contact information of their establishment or legal representative, along with any subsequent updates to this information, as stipulated in Article 4. In addition, a sanction regime to deal with possible violations of the obligations under the Directive is established[33].

The overall goal of this framework is to ensure a consistent approach to imposing obligations on both service providers and Member States in the context of electronic evidence collection in criminal proceedings, thereby overcoming challenges arising from divergent national regulations and, most importantly, from dealing with service providers that, while operating in the Union, are located outside it[34].

3. A glimpse into the past: legal and political context surrounding the Directive adoption

The Internet's borderless nature enables the global provision of web services, often bypassing the necessity for physical infrastructure or a corporate

28. Wahl 2023, pp. 165-168.

29. Directive (EU) 2023/1544, Art. 3.

30. According to Directive 2023/1544, Recital 13, the service provider should also designate an establishment in one of the Member States participating in a legal instrument referred to in the Directive.

31. Directive (EU) 2023/1544, Recital 7.

32. *Ivi*, Art 6.

33. *Ivi*, Art 5.

34. The Directive 2023/1544 is effective from 17 August 2023, with a deadline for Member States to incorporate it into national legislation by 18 February 2026.

footprint in the country where the services are accessible. Within the EU internal market, this leads to a diverse landscape of service providers: (i) those operating solely within their home Member State, (ii) those headquartered in one Member State but serving multiple others, and (iii) those located outside the EU yet offering services to one or more Member States, irrespective of their establishment within the EU.

While the Union fundamentally encourages and supports the provision of cross-border services, recognising it as core freedom, this openness poses challenges when services are misused for criminal purposes, turning platforms into critical sources for legally valid evidence in judicial proceedings. Factors such as the inherent volatility and cross-border nature of data, the widespread use of encryption software to safeguard personal information, and the control of such data by private companies create significant challenges for law enforcement and judicial authorities in identifying and collecting data crucial for investigations and criminal proceedings[35]. This is why Member States have consistently identified these challenges as critical issues requiring collective action. Such awareness particularly came to the fore in the aftermath of the terrorist attacks in Brussels, when the tragic events led to the issuance of a joint statement by Justice and Home Affairs (JHA) ministers and representatives of the EU institutions on the urgency of improving the rapid and effective acquisition of electronic evidence by enhancing cooperation with both third countries and national service providers operating on European territory[36]. The same concern was shortly thereafter reiterated in the Council conclusions of 9 June 2016, in which Member States urged the European Commission to prioritise the development of a unified EU strategy to advance criminal justice standards in the digital realm. Harmonised rules at the EU level have been increasingly seen as necessary to foster a more consistent approach to EU criminal law and to remove barriers to the provision of services, thereby improving the functionality of the internal market.

The legal landscape across the Member States has hitherto displayed significant variation in the obligations imposed on service providers, in particular with regard to access to electronic evidence in criminal proceedings, and such fragmentation has inevitably led to legal uncertainty for all stakeholders. Service providers, in particular, typically have to navigate between different and sometimes conflicting obligations and sanctioning regimes, depending on whether services are provided domestically, across borders within the EU or from external jurisdictions. Monitoring nationally applicable policies worldwide and their frequent changes is a demanding task for service providers and require constant adaptation, sometimes including the need to check regional differences within the same country. Just as challenging for the service provider is the handling of the large number of requests, which are only sometimes clear to the recipient, especially if they come from less experienced law enforcement officers. This requires contacting the authority to clarify the contents of the request and the applicable policies and requirements, with a considerable impact, given the large volume of queries they receive. Besides that, even the very authentication of incoming requests is burdensome and entails more than checking verified e-mail domains.

Of course, this burden isn't solely on the shoulders of private actors. National authorities also face a demanding and intricate situation, operating within a murky legal and operational framework. So far, as far as cross-border e-evidence collection is concerned, within the EU, two main channels have been available. The first is relying on the Convention on Mutual Assistance, which, while offering a more advanced form of cooperation compared to typical international patterns, still suffers from significant limitations stemming from the use of traditional routes. A more innovative option is the European Investigation Order (EIO) Directive, introduced in 2017. This instrument follows the mutual recognition model, empowering the issuing judicial authority to directly transmit an investigation order to the competent authority in another Member State for execution. While boasting a

35. Franssen 2024.

36. Extraordinary meeting of Ministers for Justice and Security and representatives of the EU Institutions, Brussels, 24 March 2016.

streamlined procedure and significantly reduced processing times, the EIO is not without its legal and practical challenges. Beyond the many well-known operational issues[37], the system assumes mutual trust and acceptance between the Member States in order to make this streamlined and fast mechanism work. Still, more than twenty years of practical experience in the field show that such trust and acceptance cannot be taken for granted[38]. The truth is that mutual recognition systems, although designed to be "streamlined" and function "out of diversity" perform poorly in the absence of a level playing field and are characterised by an inherent complexity. They heavily depend on the domestic setting, and EIO is no exception. All the more reason why it proves inadequate for obtaining electronic evidence, where time is of the essence.

National legal frameworks in the EU are highly nuanced. A targeted survey of public authorities in the Member States unveiled divergent approaches concerning the connecting factors used to assert jurisdiction over service providers, such as head office, service, or data location[39]. Moreover, these surveys have shed light on service providers' differing responses to requests from foreign law enforcement authorities, resulting in varying reaction times. This discrepancy stems from the diverse regulatory regimes governing whether service providers are obligated to cooperate and the potential sanctions for non-compliance. Further complicating matters are the many regimes implemented at the national level in response to the absence of a general requirement for service providers to establish a physical presence within the Union. These measures exhibit significant variability from one country to another. For instance, there are systems like the German Network Enforcement Act (NetzDG)[40], enacted in 2017, which mandates social network providers to designate a local representative tasked with managing enforcement requests and stipulates fines for non-compliance. In contrast, domestic approaches like the Belgian one do not necessitate local representation but seek to enforce national obligations directly against providers abroad through domestic legal proceedings[41].

Faced with many restrictions, the public authorities have increasingly turned to voluntary collaboration, leading to a fragmented array of informal agreements forged directly with private service providers. As of today, most collaborations between authorities and private parties for the purpose of obtaining electronic evidence are based on voluntary and informal relationships. However, even this situation is far from ideal. These arrangements pose considerable management difficulties and, most importantly, offer unpredictable results[42].

Against this general context, the groundbreaking idea of formalising voluntary cooperation between authorities and private parties at the European level has gained momentum. Central to this system is the requirement for all service providers operating in the Union to designate a specific establishment or legal representative within each Member State where they do business. This designation serves a two-fold purpose. Firstly, it ensures clear identification and proper targeting of evidence-gathering orders in criminal proceedings. Secondly, it simplifies compliance for service providers by establishing a designated contact person responsible for receiving, complying with, and executing such orders on their behalf.

While civil society organisations expressed reservations about the desirability of EU-wide legis-

37. European Judicial Network 2018. On this topic, see also: Mosna 2024; Szijártó 2023; Mitsilegas 2020; Mitsilegas 2019; Amato–Velicogna 2020; Biasiotti 2018; Bachmaier 2018; Amato–Cavallini–Carboni 2018; Sicurella 2018; Marguery 2016.

38. Lenaerts 2017.

39. SWD(2018) 118, p. 133-136.

40. Bundesministerium der Justiz, *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken* (Netzwerkdurchsetzungsgesetz – NetzDG)/*Act to Improve Enforcement of the Law in Social Networks* (Network Enforcement Act), 2017.

41. Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM(2018) 226, 17 April 2018.

42. 5th Annual SIRIUS Report, pp 72-73.

lation in this domain, preferring instead to focus EU action on enhancing mutual legal assistance procedures, stakeholders – including service providers – emphasised the importance of ensuring legal certainty in direct collaboration with public authorities and avoiding conflicts of law. This approach, on the other hand, was also advocated by public authorities during the consultation stage. Key concerns they raised during consultations included the challenges of unreliable cooperation with service providers, a lack of transparency, and legal ambiguity surrounding jurisdictional matters related to investigative measures.

Despite converging visions, the legal and political landscape surrounding this initiative was uniquely complex because of multiple factors. Notably, the Directive, which serves as a vital element of the operation of the e-Evidence package, not only intersects different layers of legislation – including national, European and international – but also touches on a broad spectrum of legal domains, ranging from judicial cooperation in criminal matters to data protection and privacy legislation. Also, its evolution has been significantly affected by the need to take into account the law of third countries, especially US law, as major service providers holding crucial evidence fall under its jurisdiction. This nuanced set-up has brought to light the formidable challenges of aligning legal frameworks and ensuring coherent interactions between different jurisdictions' regulatory systems.

4. Clashing priorities and founding common grounds: the institutional discourse towards a balance between security and fundamental rights

The Directive – together with the Regulation – is the result of intense and challenging negotiations. It impacts the field of judicial cooperation with an unprecedented approach that, more than any other instrument in the field, puts the principle of mutual trust to the test. This legislative package offers new possibilities for authorities to pursue criminal investigations that require acquiring electronic evidence across borders. It streamlines processes, thereby navigating challenges inherent in interactions with foreign jurisdictions – challenges that cooperation mechanisms currently in place[43] often find insurmountable. These include the common occurrence of service providers denying access to requested data – either because the requesting authority lacks jurisdiction over the service provider's headquarters location or due to the nationality of the individual whose data is sought – and the unavoidable delays brought on by applying judicial cooperation procedures. Both conventional methods and those founded on the principle of mutual recognition necessitate the participation of the authorities from the State being asked for cooperation, resulting in timeframes that are starkly at odds with the ephemeral nature of electronic data.

The new e-Evidence package was designed precisely to move beyond the constraints of currently available legal instruments and to enhance clarity and legal certainty while significantly expediting the process of obtaining electronic evidence. It imposes an obligation on service providers to respond within 10 days (and, in an emergency, within 8 hours)[44], which is a very tight timeframe compared to the 120-day deadline stipulated in the EIO Directive and, above all, to the average 10 months in traditional mutual legal assistance procedures. This oversimplification, however, makes it all the more difficult to strike an inherently fragile balance between the need to facilitate law enforcement and prosecution in a digital environment on the one hand and the protection of privacy and the other rights of suspects and accused persons on

43. Within the EU legal framework, the cross-border collection of electronic evidence is governed by several legal instruments, including Directive 2014/41/EU on the European Investigation Order in criminal matters, the Council Framework Decision of 13 June 2002 on Joint Investigation Teams, the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, Regulation (EU) 2018/1727 on the European Union Agency for Cooperation in Criminal Justice (Eurojust), Regulation (EU) 2016/794 on the European Union Agency for Law Enforcement Cooperation (Europol). The matter is also governed by the Mutual Legal Assistance Agreement between the European Union and the United States of America.

44. Regulation (EU) 2023/1543 of the European Parliament and of the Council 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, Art. 10 (3) and (4).

the other hand[45]. This issue becomes evident when examining the intricacies and debates that characterised the process of establishing the new rules[46].

When the European Commission published its legislative proposal after an extensive two-year preparation process, the new system was met with a mix of support and concerns. On the one hand, key European entities recognised the need for faster access to evidence while strongly emphasising the importance of safeguarding rights. The European Economic and Social Committee (EESC), for instance, highlighted the need for legal representatives within the Union[47], while data protection bodies like the European Data Protection Board (EDPB)[48] and the European Data Protection Supervisor (EDPS) insisted on aligning the new rules with existing data protection laws. They also called for robust safeguards, including judicial oversight and adherence to the Court of Justice of the European Union's (CJEU) case law, to ensure individuals' rights are protected in the process[49]. This strong commitment to fundamental rights was strongly embraced by the European Parliament, which, throughout the legislative process, maintained a highly critical stance on this instrument. On the other hand, the European Council[50] emphasised the critical need for rapid cross-border access to electronic evidence to effectively fight terrorism and organised crime, particularly in light of the US Cloud Act[51], which accentuated the necessity for a cohesive EU strategy to negotiate a binding agreement with the other side of the Atlantic. The same orientation was ultimately adopted by the Council of Ministers, though through a convoluted process[52].

Interinstitutional negotiations started in early 2021 under the Portuguese Council presidency, marked by profound differences between the text of the Council's general approach and the EP's position. After many moments of stalemate, which at times seemed insurmountable, discussions intensified under the French and Czech presidencies. On 29 November 2022, after eight trilogues, the co-legislators reached a political agreement on the most controversial elements of the two proposals. On 25 January 2023, the Council confirmed the agreement with the Parliament and at the end of the same month, the committee approved the agreed text, which was adopted in plenary on 13 June 2023. The final text of both legal tools is not so far from the Commission's original proposals in substance, reflecting a shared belief that more effective legislation is needed to handle cross-border electronic evidence. Nevertheless, the journey towards the adoption of the e-Evidence package was long and marked by intense debate, with deeply

45. Sippel 2023, p. 109; Forlani 2023; Tosza 2023; Christakis 2019.

46. COPEN Technical Working Group on 27 April 2018 under the Bulgarian Council presidency.

47. European Economic and Social Committee, Opinion on the 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 – 2018/0108(COD)] and on the Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings [COM(2018) 226 – 2018/0107(COD)], 12 July 2018.

48. European Data Protection Board, Opinion of the EDPB on Commission proposals of the EP and of the Council on European production and preservation orders for electronic evidence in criminal matters, Brussels, 18 October 2018 (OR. en), 13317/18.

49. European Data Protection Supervisor, EDPS Opinion on Proposals regarding European Production and Preservation Orders for electronic evidence in criminal matters, Opinion 7/2019, 6 November 2019.

50. Justice and Home Affairs Council, 11-12 October 2018.

51. The U.S. government adopted the Clarifying Lawful Overseas Use of Data (CLOUD) Act in March 2018 to speed up access to electronic information held by U.S.-based global providers that are critical to foreign partners' investigations of serious crime, ranging from terrorism and violent crime to sexual exploitation of children and cybercrime.

52. Council of the European Union, Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters – general approach, Brussels, 12 December 2018 (OR. en), 15292/18. Ultimately, the Council agreed on its position on the Directive on March 8, 2019. See: Justice and Home Affairs Council, 7-8 March 2019.

divided opinions and significant deadlocks that, at times, suggested that the proposals might be abandoned.

4.1. Institutional deadlocks and breakthroughs: towards a unified approach

After the European Commission introduced its legislative proposal in April 2018, the Council moved relatively quickly to agree on its general approach, adopting positions on the draft Regulation in December 2018 and on the draft Directive in March 2019. Yet, these milestones belied the contentious negotiations underlying the process. Within the Council of Ministers, Member States were divided from the outset[53]. While some supported the Commission's proposals, even advocating for stricter measures – such as real-time monitoring of communication data from emails and messaging platforms for criminal investigations – others were more critical[54]. The dissenting Member States highlighted a lack of sufficient checks and balances in the proposals and expressed concern about the inadequate protection of fundamental rights, underlining the difficulties in crafting legislation acceptable to all parties.

Although the Council reached a general consensus on the legislative approach, the divisions within its ranks were far from resolved. This was evident when eight Member States formally declared their non-support for the compromise proposals[55]. The reservations held extended beyond a general apprehension about the uneven application of the rule of law across the EU[56]. They specifically argued that the compromise proposal fell short of addressing their concerns about the effectiveness of the proposed notification systems. They questioned the ability of the executing State to refuse recognition of an order if there are well-founded reasons to do so. Particularly, there was a call for more robust safeguards, especially concerning orders related to highly sensitive data[57]. These concerns persisted even after interinstitutional negotiations began in January 2021. While a joint position aligned with the Council's general approach eventually emerged, this only occurred after intense debate, due in part to the European Parliament's staunch resistance to certain compromises.

As far as the proposal for a Directive is concerned, national JHA ministers within the Council retained the Commission's criteria regarding the location of legal representatives while incorporating further details on various aspects. These include the extent of their responsibilities, the resources and authority they must possess, the specific duties they are accountable for, and the penalties for non-compliance. Moreover, a significant emphasis was placed on ensuring that these legal representatives could be promptly identified and contacted by the requesting authority[58].

The European Parliament's position, which crystallised in December 2020, added further complexity to the legislative process. Building on preparatory work by the LIBE Committee, the Parliament introduced 841 amendments to the draft Regulation, proposing sweeping changes to its core provisions[59].

At the heart of these amendments was a stronger emphasis on the notification mechanism. Debates centred on whether the Member State hosting the

53. COPEN Technical Working Group on 27 April 2018 under the Bulgarian Council presidency.

54. Justice and Home Affairs Council, 4-5 June 2018, Luxembourg. Ministers from Belgium, Portugal, Cyprus, France, Greece, Italy, and Estonia spoke out to insert a measure into the bill to allow authorities to intercept communication in real-time.

55. Justice and Home Affairs Council (Justice) at the European Council in Brussels, Belgium, 7 December 2018. Germany, the Netherlands, Hungary, Sweden, Finland, Greece, Latvia, and the Czech Republic all voted against.

56. In particular, German Justice Minister Katarina Barley expressed concern that the rule of law is not respected equally throughout the European Union. Cft. Stolton 2018.

57. Letter to Ms Věra Jourová European Commissioner for Justice, Consumers and Gender Equality from the Ministers of the Netherlands, Germany, Czech Republic, Finland, Latvia, Sweden, Hungary, Hellenic Republic.

58. Justice and Home Affairs Council, 7-8 March 2019.

59. European Parliament, Report – A9-0256/2020 of 11 December 2020: Report on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters.

service provider or legal representative should play a role in reviewing orders, the specific categories of data subject to such scrutiny, and the scope of the authority's capacity to refuse requests. The Parliament also proposed additional prerequisites for issuing orders, along with a comprehensive list of refusal grounds, some of which would be mandatory[60].

In addition, the Parliament questioned the necessity of the Directive, suggesting that elements of it be incorporated into the Regulation to streamline the legislative framework. This suggestion arose from concerns over the Regulation's legal foundation and the perceived redundancy of the Directive, which required all EU Member States to designate a legal representative, regardless of their participation in the legal frameworks outlined in Title V, Chapter 4, of the Treaty on the Functioning of the European Union (TFEU). The Commission's proposal to potentially expand the role of these legal representatives in future instruments was seen as exceeding its intended scope, raising doubts about its compatibility with Articles 53 and 62 TFEU. Consequently, the Parliament argued that only Member States participating in the Regulation should be required to appoint legal representatives. In response to these critiques, key aspects of the Directive were incorporated directly into the Regulation as a complementary measure under Article 82 TFEU, reflecting the Parliament's strategic efforts to align the legislative framework with its broader vision and legal interpretations.

Interinstitutional negotiations required concessions on both sides. In the second half of 2021, the Council introduced changes to its general approach, thus demonstrating a willingness to compromise beyond its initial position. The adjustments initially brought in (supported by the Member States only as a measure of last resort to overcome the negotiating impasse) did not remove the concerns of the Parliament regarding fundamental rights; therefore, in an attempt to overcome the stalemate, a number of new compromise proposals on the most contentious issues were subsequently tabled. At the same time, previously unresolved issues were revisited. In particular, the resumption of discussions on the draft Directive was promoted, with a view to emphasising the need for its provisions to be kept separate. The conversation was fruitful and resulted in an outcome that gained the approval of the European Parliament. After eight trialogues, and despite the lingering profound disagreement on many crucial issues, the intense negotiating efforts of both the European Parliament and the Council made it possible to reach a political agreement on a final compromise version drafted in late 2022 that gained the support of the Member States delegations and the European Parliament in 2023.

5. A peek into the future. From blueprint to reality: navigating the operational challenges on the Directive roll-out and implementation

Experts, academics, and stakeholders welcomed the adoption of the e-Evidence package, among whom there is consensus that it is a milestone in the collaboration between authorities and service providers. Most service providers have also valued the new rules. They see them as bringing much-needed legal certainty to the process of disclosing data in criminal investigations. The new system will eliminate or significantly reduce the current burden they face in assessing the legitimacy of each request as, previously, service providers had to navigate a complex legal landscape with many applicable national laws and international instruments. Furthermore, the standardisation of the format for data disclosure and retention orders has been widely praised for its positive impact on managing these requests at an operational level[61]. Nevertheless, many voices have been and still are critical of the overall new system of access to e-evidence. Beyond the delicate balance of competing interests[62], doubts indeed arise as to the system's practical viability, in respect of which the successful implementation of the Directive and the smooth functioning of the decentralised IT system are prerequisites.

Notably, three primary challenges are supposed to hinder the successful implementation of this system: (a) the organisational and techni-

60. Christakis 2023.

61. 5th Annual SIRIUS Report, p 75.

62. Berthélémy 2023; Tosza 2021; Tosza 2024; Mitsilegas 2018.

cal capacity of the service providers, specifically their appointed offices and legal representatives, required to intervene in the procedure envisaged by the e-evidence package; (b) underlying issues related to the effective functioning of certain operational and technical tools designed to support the procedures; and (c) the complex interplay of legal frameworks of collaboration that affect the overall effectiveness of the system.

5.1. Designated establishments and legal representatives' organisational and technical capacity

Several factors can influence the organisational and technical capacity of designated establishments and legal representatives (see Tab. 1). Key among these are ambiguities in the relevant regulations together with financial and non-economic burdens associated with managing procedures. Problems with substantial operational repercussions are likely to be caused by the unclear rules establishing the criteria for determining the designated establishment or legal representative. The Directive mandates that service providers, including those outside the EU, establish them within the Member States territory so as to ensure accessibility for requests by foreign authorities regarding the production or preservation of e-evidence. Guidance on how to identify these establishments or representatives, however, is so far missing, thus allowing discretion and leading to uncertainty for companies. According to the Directive, a "substantial connection" to the Member States where services are offered is pivotal for determining the service provider's obligations. Yet, defining what a "substantial connection" actually is remains ambiguous, especially in cases where the service provider does not have a physical establishment in the Member State. The criteria hinge on having a significant user base or targeting activities towards one or more Member States, both vaguely defined. In the Impact Assessment, the option to specify a "significant user base" was considered but ultimately discarded due to challenges in setting and applying a specific threshold and the risk of creating exploitable loopholes, suggesting a preference for inclusiveness. Similarly, the determination of "targeting of activities" is subject to unclear factors[63]. Consequently, service providers face uncertainties in determining their obligations under the Directive and understanding sanctions, potentially leading to inconsistent compliance and enforcement of the Directive's requirements.

Alongside this, operational challenges are likely to arise due to the financial and non-financial burdens that fulfilling the obligations of the new e-evidence collection system will entail, particularly for non-EU SMEs. While direct cooperation with private entities is designed to cut costs and boost efficiency, the transition to this new collaborative framework will impose a higher financial burden on these private actors. Consider, for instance, the costs associated with designating entities under Directive 1544/2023/EU within the EU. Even though "the designated establishment or legal representative may be shared among several service providers, particularly SMEs"[64], this approach could still impose a significant burden on the business community. Service providers must cover all expenses related to the establishment, maintenance, and management of their legal representative or designated establishment to ensure compliance with the Directive. This includes costs for data transmission or backup, with the possibility of reimbursement dependent on the laws of the issuing state allowing such reimbursements for similar national orders[65].

Both financial and non-financial burden is also expected to adjust private entities' structures to comply with requests from other Member States' authorities, in accordance with the stipulated regulations[66]. Immediate and comprehensive responses to authority requests require stringent technical procedures and a skilled team ready to meet tight deadlines[67], all the more so that poten-

63. Regulation (EU) 2023/1543, Art. 3 (4) lett b; Recital 30.

64. Directive (EU) 1544/2023, Recital 7.

65. Regulation (EU) 2023/1543, Art. 14; Recital 68.

66. SWD(2018) 118. See also: Cuadrado Salinas 2023.

67. Juszczak–Sason 2023, pp. 182-200; Schauenburg–Zapf–Rossbrey–Málaga 2023.

Category	Key Issues	Operational Implications
Regulatory Ambiguities	- *Unclear designation criteria*: Ambiguous rules on how to identify a legal representative or designated establishment. • "Substantial connection" dilemma; • Vague "user base"/"targeting" criteria.	- *Uncertain obligations and sanctions*: Providers struggle to understand their exact responsibilities and risk inconsistent enforcement. - *Discretion in application*: Divergent interpretations can lead to uneven compliance and potential legal disputes. - *Higher legal risk*: Inability to pinpoint when penalties might apply or which criteria trigger full Directive obligations.
Financial/Non-Financial Burdens	- *Establishment and maintenance costs*: Setting up and running a designated establishment or legal representative entails fees for infrastructure, staffing, and administration. - *Potential reimbursement gaps*: Whether costs (e.g., data transmission, backup) are recoverable depends on national laws. - *Particular strain on SMEs*: Shared representatives are allowed but may still impose considerable overhead. - *Non-economic burdens*: Internal reorganisations, compliance procedures, and increased documentation demands add to the overall load.	- *Heightened financial strain*: Smaller companies or non-EU entities risk higher cost impacts, including fines for non-compliance. - *Vulnerability to penalties*: Even minor infractions can trigger sanctions that can weigh heavily on SMEs.
Technical Capacity	- *Stringent demands and Directive's silence on technical standards*: Specific expertise is needed to identify problematic aspects, challenge unjustified requests and navigate diverse legal frameworks for electronic evidence.	- *Complex compliance architecture*: Heightened administrative burdens and coordination challenges arising from the need of continuous adaptation to multiple legal frameworks and potential confusion about standards of proportionality and necessity.
Skills	- *Multidisciplinary expertise*: Beyond legal know-how, technical and linguistic proficiency is needed to review requests accurately, including verifying certificates and documentation. - *Limited support networks for private actors*: Companies lack the resources available to national authorities (e.g., established liaison channels and networks).	- *Higher demand for specialized staff*: Legal representatives or designated establishments must detect problematic requests and raise challenges where necessary. - *Steep learning curve for SMEs*: Smaller businesses can face disproportionate difficulty acquiring the mix of legal, technical, and language skills. - *Potential for procedural bottlenecks*: Inadequate expertise can delay or derail the timely exchange of information, increasing the risk of fines or legal disputes.

Tab. 1 — *Organisational and Technical Capacity Challenges from an Operational Perspective*

tial violations can result in financial penalties[68]. These penalties, while perhaps a minor deterrent for large companies like Google, could impose a disproportionate financial strain on smaller com-

68. Cuadrado Salinas 2023.

panies[69]. Additionally, designated establishments or legal representatives who are jointly and severally liable with service providers cannot invoke unauthorised data transmission or inadequate internal procedures as a defence against non-compliance.

While the Directive fails to detail technical capacity requirements, legal representatives or designated establishments must possess specific expertise to identify any problematic aspects of requests and challenge, where appropriate, any foreign authority request that may seem unjustified or potentially infringe on privacy due to governmental overreach[70]. Navigating this complex landscape is challenging, especially with different prerequisites for issuing orders[71] and the absence of explicit justifications for proportionality and necessity in some cases[72]. The "variable geometry" of prerequisites for issuance and guarantees of proportionality and necessity introduces diverse coordination patterns and potential administrative burdens arising from managing different national frameworks for obtaining electronic evidence[73].

Yet there is a further level of complexity to consider, especially when it comes to the technical skills of those who perform these procedures. The expertise required to conduct such operations is not merely legal. While tasks such as discerning the legitimacy of a certificate or identifying problems in received documentation are generally acknowledged as challenging, particularly in a multilingual context, it is often overlooked that in managing cross-border cooperative procedures, seemingly trivial practical issues can be even more insidious. Decades of experience with mutual recognition cooperation models have revealed numerous difficulties inherent in these processes, which are likely to be even more severe for private entities lacking the substantial expertise, resources, and support networks available to judicial and police authorities since the adoption of the European Arrest Warrant.

5.2. Shortcomings in operating and technical support tools

The e-Evidence package introduces essential operational support tools to make carrying out application and compliance procedures feasible. However, inherent systemic issues make using these tools challenging (see Tab. 2).

A particularly relevant example in this context is Article 4(4) of the Directive, which mandates the creation of a repository on the European Judicial Network's webpage. Member States are required to compile information about the establishments and legal representatives designated by service providers, including contact details, accepted receiving languages, and the precise territorial scope when a service provider designates multiple establishments or appoints multiple legal representatives. This measure is welcome, as the creation and maintenance of a dedicated repository is essential to enable competent authorities to identify the correct recipient, thereby ensuring the functionality of the system, especially when a service provider has multiple establishments or representatives. Yet, this represents a typical illustration of a seemingly simple but practically demanding operational challenge. The establishment of effective national notification systems between service providers and central authorities cannot be taken for granted. Recent research project findings reveal the complexities involved in what may seem like

69. Article 5 of the Directive mandates that Member States set up a system of "effective, proportionate, and dissuasive penalties", which, according to Regulation Article 15, could include fines of up to 2% of a service provider's total annual worldwide turnover from the previous year. Still, the absence of detailed guidelines on what constitutes "effective, proportionate, and dissuasive penalties" may result in inconsistent application across the EU. This inconsistency could lead to legal uncertainties for businesses operating in multiple Member States, fostering varied compliance challenges and escalating operational costs. Moreover, this ambiguity could weaken the Directive's effectiveness, as insufficient deterrent penalties might fail to encourage compliance, complicating enforcement efforts further.

70. Art. 11 (4) Regulation EPOC. See Sarkowicz 2022, pp. 101-110.

71. Regulation 1543/2023/EU, Art. 5 (2) and Art. 6 (2).

72. Busillo 2023.

73. *Ibidem*.

Category	Key Shortcomings	Operational Impact
Systematising Contact Details (Repository)	- *Complexity of Article 4(4) repository*: Although seemingly straightforward, setting up and maintaining accurate contact details databases of service providers can be demanding and challenging in practice.	- *Potential for misdirected or delayed requests*: If repository data are incomplete or outdated, authorities can struggle to identify the correct recipient. - *Increased administrative overhead*: Providers and authorities must devote time and resources to keep listings accurate and current. - *Risk of partial or ineffective solutions*: Without fully addressing underlying complexities, any repository-based tool might fail to function as intended across different Member States.
Decentralised IT System Functioning	- *Limited e-CODEX deployment:* Many Member States lack an operational access point for new procedures. - *Volume constraints*: e-CODEX sets size limits on data transmission, requiring alternative channels for large data sets. - *Rapidly evolving requirements*: Technological advances and shifting legal frameworks can outpace the integration process if not proactively managed.	- *Delayed or incomplete data exchanges*: Without fully configured access points or alternative channels, transmitting electronic evidence promptly can be difficult. - *Challenges for private actors (SMEs in particular)*: Adapting to e-CODEX and related systems demands specialised IT capacity and resources. - *Escalating costs and compliance risks*: Entities that postpone updating or expanding their technical infrastructure may face higher expenses and potential penalties by the end of the implementation period.

Tab. 2 — *Shortcomings in Operating and Technical Support Tools*

the straightforward technical task of creating databases for the electronic addresses of authorities responsible for executing orders (e.g., EIO)[74]. These insights highlight that such informative tools are not merely technical solutions but involve IT, legal, and organisational dimensions influenced by various non-technical and contextual factors. A comprehensive understanding of these elements is vital to develop the system effectively for its intended use and ensure its relevance in a rapidly evolving technological and societal landscape.

Along with this, it's crucial to acknowledge the potential difficulties in aligning the IT systems of designated establishments and legal representatives with the decentralised IT system used for secure communications and exchanges, likely to be e-CODEX. Designed as a content-neutral e-delivery platform, e-CODEX integrates with existing national and European e-Justice IT systems rather than replacing them[75]. While this theoretically simplifies access and use, practical challenges remain, especially as the e-evidence system expands access to private entities. To begin with, each e-CODEX participant requires an access point to join the network. This access point can either be the one provided by the Commission or an alternative at the national level. However, many Member States currently lack an access point and still necessitate gateway connector installation by trusted authorities. Even when a national access

74. See, for instance, the results of the CCDB Project, which was launched to establish an EU Criminal Court Database (CCDB) by collecting contact data on all judicial bodies of the Member States and project partners States responsible for proceedings related to issuance of EIOs.

75. Regulation (EU) 2022/850 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-CODEX system). See: Ontanu 2023; Velicogna–Steigenga–Taal–Schmidt 2020; Velicogna 2018.

point is available, it must be configured for specific cooperative procedures, currently available only for the EIO[76]. Furthermore, two additional considerations must be addressed. The first concerns the contact list that the authority must use to forward communications and requests to private parties. It is not sufficient for this list to be merely available on the European Judicial Network's dedicated page. For the authority to be able to use this directory to send requests or communications, it needs to be integrated with the e-Codex system. Secondly, while the e-CODEX system is primarily designed for the exchange of communications, data exchange is possible only if it does not exceed a certain volume. Therefore, a different channel will be necessary for transmitting larger volumes of data. In conclusion, proactively addressing technical and usability issues is crucial to avoid potential costs and non-compliance problems at the end of the three-year implementation period.

5.3. Interplay with other legal instruments

While not the main focus of this article, it's important to recognise that the complex international legal landscape could have operational implications (see Tab. 3). Notably, the e-Evidence package fits into a broader array of national, regional, and international mechanisms that integrate the private sector into government crime-fighting initiatives[77]. As such, the e-Evidence package is designed to complement existing legal frameworks, leading to various patterns of cooperation[78], though the specifics of its interaction with these frameworks are yet to be defined.

In this respect, the interaction between the EIO Directive with Directive 1544/2023 warrants particular attention. Judicial authorities in the Member States retain discretion in selecting the most suitable instrument for each case, potentially preferring the EIO for its extensive scope in requiring the production of digital evidence, among other investigative measures. However, it must be noted that the EIO Directive offers limited details on accessing electronic evidence. Furthermore, requests for evidence via the EIO cannot bypass inter-authority collaboration, as they must adhere to the mutual recognition instruments' standard procedure. For service providers, the enforcement request for the EIO originates from the executing authority in the host country of the legal representative or designated establishment following a prior evaluation. This multi-tiered process may pose challenges for executing requests, especially given the varying cooperation modes and responsibilities imposed on the provider.

A further critical limitation of the Directive is its actual inability to address challenges stemming from the domestic laws of non-EU service providers. Notably, "blocking statutes" such as those within the U.S. Electronic Communications Privacy Act, which restrict U.S. service providers from sharing content data with foreign authorities, significantly hinder cooperation with EU law enforcement[79]. The European Commission acknowledges this hurdle, emphasising its persistence until a bilateral U.S.-EU agreement is established. This situation underscores the intricate interplay between international law and national legal frameworks governing cross-border data access and transfer[80]. A pivotal development in this sphere is the U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act, enacted in 2018. This legislation empowers the U.S. to negotiate "executive agreements" with foreign countries, facilitating reciprocal access to data held by each nation's service providers. Such agreements would authorise U.S. service providers

76. The EU has employed Reference Implementation Software in criminal proceedings, notably for the European Investigation Order (EIO) as part of the e-EDES Infrastructure, which operates on the e-CODEX platform. In the civil sphere, comparable tools are under development to support the revised regulations for the Service of Documents and the Taking of Evidence. These initiatives include the creation of the Reference Implementation Software for the Service of Documents (SoD) and for Taking of Evidence (ToE). See Ontanu 2023, p. 96 ss.

77. Brière 2021; González Fuster–Vázquez Maymir 2020; Signorato 2023; Mitsilegas 2014.

78. Directive 1544/2023/EU, Art. 1.

79. Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters. Explanatory Memorandum, Strasbourg, 17 April 2018, COM(2018) 225, 2018/0108(COD), p. 11.

80. Franssen 2018.

Category	Key Points	Operational Implications
Interaction with EU Instruments	- *Broader legal ecosystem*: The e-Evidence package complements existing EU frameworks, though exact cooperative patterns remain to be clarified.	- *Choice of instrument uncertainty*: Service providers must respond differently depending on whether authorities use the EIO or e-Evidence procedures, creating administrative complexity. - *Parallel obligations*: Overlapping requirements can cause confusion regarding enforcement and responsibilities.
Interaction with Non-EU Instruments	- *Blocking statutes*: Certain non-EU laws prohibit service providers from sharing content data with foreign authorities, limiting compliance with EU demands.	- *Legal conflicts for providers and continued uncertainty*: Non-EU companies may be unable to comply with EU orders if barred by home-country laws, risking enforcement deadlock and potential liability on both sides. Service providers can face ambiguous obligations when data are stored under differing legal regimes.

Tab. 3 — *Interplay with Other Legal Instruments*

to comply with valid legal requests from partner countries for content data. Negotiations for a similar EU-U.S. agreement commenced in 2019 but were temporarily suspended to align with European electronic evidence legislation. Resuming in 2023, these talks remain complex and uncertain as both parties grapple with the prospect of potentially relinquishing sovereign data access rights, irrespective of data location[81].

6. Conclusions

A substantial part of criminal investigations in the EU today necessitates access to information found on online platforms like communication services, social networks, and marketplaces. However, authorities face significant challenges in obtaining such cyber evidence due to its transient nature and the frequent need for cross-border cooperation, as the data are often stored abroad or managed by foreign service providers. Essentially, when dealing with electronic evidence, cross-border cooperation reaches the highest levels of complexity, as beyond the usual difficulties inherent in such collaborations, the nature of electronic evidence introduces further complications. Its volatility and susceptibility to alteration or deletion make the timing of evidence collection even more crucial.

Although a major effort has been made to streamline cross-border judicial cooperation over the past two decades, law enforcement and judicial authorities still encounter significant challenges in accessing electronic evidence. Even state-of-the-art instruments based on the principle of mutual recognition have struggled to keep up with the challenges posed by new digital evidence. Not surprisingly, the direct authority-to-authority dialogue, mandated to conclude within the three-month timeframe established by the EIO, has proven ineffective in a field where time is of the essence.

In addressing these challenges, authorities have increasingly turned to informal partnerships with private service providers. However, this unregulated approach, while seemingly more effective on paper, presents complications for both the requesting and requested parties. Cooperation for obtaining electronic evidence occurs within a cumbersome and diverse legal landscape, as domestic systems differ significantly in key areas (e.g., jurisdictional linkage factors, obligations to provide necessary information, sanction structures, and mandates for companies to establish local offices). This diversity leads to inconsistent obligations for recipients, which affects response times to evidence-collection

81. Bachmaier 2023; Propp 2023.

requests and the willingness to cooperate. Moreover, it creates uncertainties about the admissibility of any obtained evidence, further complicating the efforts of authorities.

The pressing need to move beyond these limitations has sparked a vigorous debate in the EU, prompting the European Commission to come up with effective legislative solutions aimed at offering greater clarity and certainty in the cross-border evidence-collection process. As a result of two years of work, a highly innovative proposal for a legislative package was brought forward to respond to this sense of urgency. The proposed new system for e-evidence gathering relied on the architecture of the most advanced cooperative tools based on the principle of mutual recognition, standardising processes, conditions, and templates, but it went much further. It envisioned more streamlined procedures and very short response times and, most importantly, established unprecedented legal bases for formalising direct dialogue between judicial authorities and private actors. Although much-awaited, the proposal was met with conflicting reactions, which were very clearly echoed during the negotiation process, which was anything but smooth. The discourse surrounding the e-Evidence package has been heated. The new system's plan for oversimplification sparked criticism and caused a significant rift among institutions concerning the issues that could arise from the fragile balance between the need for rapid investigative activities and the rights of the accused. Despite these clashing perspectives and the many moments of seemingly insurmountable deadlock, the collective agreement on the need for more effective measures in this area prevailed, and a final solution was achieved that remains fairly close to the initial proposal.

Mirroring previous mutual recognition instruments in the field of judicial cooperation, the new system creates a defined cooperative path between requesting and requested parties for the delivery of EPOCs or EPOC-PRs, i.e., standard certificates with which it is possible to request the production of evidence or its preservation, depending on the case. The response time is very short, in urgent cases even just a few hours, and the reasons that recipients can use to refuse compliance are very limited. Moreover, there is a penalty regime in case of non-compliance, which should discourage divergent behaviour.

Particularly noteworthy for this analysis are the requirements outlined in Directive (EU) 2023/1544 and the provisions within the Regulation mandating the use of a decentralised IT system for exchanging communications and documentation between parties involved. Organisation and technology are indeed pivotal factors for the deployment of these procedures. Previous research in the field of EU judicial cooperation, after all, has long indicated that relying solely on legal remedies cannot be sufficient to close the enforcement gaps of mutual recognition instruments, and the new e-Evidence package is by no means an exception.

In this context, the Directive's requirement for service providers to designate establishments or legal representatives within the EU is crucial for ensuring the effective transmission and execution of EPOCs and EPOC-PRs. This requirement becomes particularly significant when dealing with non-EU companies operating in the European market. While the Regulation defines the procedural steps, conditions, and requirements, the Directive makes these procedures practical by identifying the responsible parties. It clarifies who will receive, execute, and be held accountable for requests, thereby enhancing enforcement, oversight, and compliance with the EU Regulation. Though not explicitly aimed at consumer protection, these measures contribute to a more regulated and transparent environment, indirectly supporting consumer interests by ensuring adherence to EU standards. Furthermore, mandating electronic transmission as the designated cross-border communication route, rather than an optional method, is a positive development. Digitising the process with state-of-the-art IT solutions promises operational benefits, including a more streamlined, secure, and reliable exchange of information. The Regulation's requirement for digital communication aligns with broader efforts to modernise and improve cross-border judicial processes. This shift towards digital systems, such as e-CODEX, is expected to enhance efficiency, resilience, and cost-effectiveness by replacing traditional paper-based methods. Managed by eu-LISA, these systems ensure interoperability, protect data, and maintain confidentiality, supporting more sustainable and efficient operations and contributing to the rapid resolution of cross-border civil and criminal cases.

Nevertheless, these key operational components come with their own set of critical challenges, particularly at the system level, where they can compromise overall functionality and effectiveness. Beyond issues arising from the interaction between the e-Evidence package and the existing legal framework, as well as limitations due to conflicts of law, there are two main sets of challenges likely to impact the practical feasibility of the new system. First, there are concerns about the capacity of private actors, especially smaller service providers, to effectively respond to cooperation requests. These challenges stem from unclear regulations, financial and operational burdens, and technical complexities. The complexity of cross-border cooperation procedures can be overwhelming for inadequately equipped private entities, potentially leading to paralysing effects and exposure to penalties. Additionally, there are issues related to the operational and technical support tools created by the legislation to support the system. Although these tools are intended to serve an enabling or supplementing function, they themselves may be difficult to implement. Examples include the creation of the European Judicial Network's repository and its integration into the decentralised IT system architecture, as well as ongoing functionality problems with the e-CODEX system.

In essence, the success of the new cross-border electronic evidence collection system is likely to depend on how effectively various operational aspects are managed. This includes addressing measures that may appear minor or straightforward but are, in reality, pivotal to the system's overall viability. Properly handling these details can be key for ensuring the system's functionality and effectiveness.

References

R. Amato, D. Cavallini, N. Carboni (2018), *Italian National Report*, in T. Marguery (ed.) "Mutual Trust under Pressure, the Transferring of Sentenced Persons in the EU: Transfer of Judgments of Conviction in the European Union and the Respect for Individual's Fundamental Rights", Wolf Publications, 2018

R. Amato, M. Velicogna (2020), *Encoding Cross-Border Judicial Cooperation in Criminal Matters: Current Practices and the Rise of the EU E-Justice Infrastructure*, in C. Billet, A. Turmo (eds.), "Coopération opérationnelle en droit pénal de l'Union européenne", Bruylant, 2018

L. Bachmaier (2023), *Mutual Admissibility of Evidence and Electronic Evidence in the EU. A New Try for European Minimum Rules in Criminal Proceedings?*, in "Eucrim: the European Criminal Law Associations' forum", 2023, n. 2

L. Bachmaier (2018), *Mutual Recognition and Cross-Border Interception of Communications: The Way Ahead for the European Investigation Order*, in C. Brière, A. Weyembergh (eds.), "The Needed Balances in EU Criminal Law: Past, Present and Future", Hart Publishing, 2018

D. Ben Miloud, C. Nicolau (2023), *e-Evidence Digital Exchange System (eEDES)*, in M.A. Biasiotti, F. Turchi, "European Investigation Order. Where the Law Meets the Technology", Springer, 2023

C. Berthélémy (2023), *e-Evidence compromise blows a hole in fundamental rights safeguards*, in "European Digital Rights (EDRI)", 2023

M.A. Biasiotti (2018), *Present and Future of the Exchange of Electronic Evidence in Europe*, in M.A. Biasiotti, J.P. Mifsud Bonnici, J. Cannataci, F. Turchi (eds.), "Handling and Exchanging Electronic Evidence Across Europe", Springer, 2018

M.A. Biasiotti, F. Turchi (eds.) (2023), *European Investigation Order. Where the Law Meets the Technology*, Springer, 2023

S. Busillo (2023), *Conservazione e produzione della prova digitale nella nuova disciplina europea: il potenziale disallineamento con i principi espressi dalla giurisprudenza di settore*, in "Freedom, Security & Justice: European Legal Studies", 2023, n. 3

C. Brière (2021), *EU Criminal Procedural Law onto the Global Stage: The e-Evidence Proposals and Their Interaction with International Developments*, in "European Papers", vol. 6, 2021, n. 1

F. Casino, C. Pina, P. López-Aguilar et al. (2022), *SoK: cross-border criminal investigations and digital evidence*, in "Journal of Cybersecurity", vol. 8, 2022, n. 1

T. Christakis (2023), *From Mutual Trust to the Gordian Knot of Notifications: The EU E-Evidence Regulation and Directive*, in V. Franssen, S. Tosza (eds.), "The Cambridge Handbook of Digital Evidence in Criminal Matters", Cambridge University Press, 2023

T. Christakis (2019), *E-evidence: the way forward* (Summary of the Workshop held in Brussels on 25 September 2019), in "European Law Blog. News and Comments on EU Law", 2019

Council of Europe (2023), *T-CY Guidance Note #13, The scope of procedural powers and of international cooperation provisions of the Budapest Convention*, 27-28 June 2023

Council of Europe (2022), *Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence* (CETS No. 224), 2022

C. Cuadrado Salinas (2023), *La Directiva Europea y las Órdenes de Producción y Conservación de pruebas electrónicas en los procesos penales. ¿Nuevas perspectivas?*, in "Ius et Scientia", vol. 9, 2023, n. 2

European Commission (2023), *Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines*, Brussels, 25 April 2023

European Judicial Network (2018), *51st EJN Plenary meeting – Conclusions on the application of mutual recognition instruments*, Brussels, 5 December 2018 (OR. en), 14754/18

Europol – European Union Agency for Law Enforcement Cooperation (2024), *5th Annual SIRIUS EU Electronic Evidence Situation Report*, The Hague, November 2023 (updated version 11 April 2024)

G. Forlani (2023), *The E-evidence Package. The Happy Ending of a Long Negotiation Saga*, in "Eucrim: the European Criminal Law Associations' forum", 2023, n. 2

V. Franssen (2024), *Cross-border Gathering of Electronic Evidence in the EU: Toward More Direct Cooperation under the e-Evidence Regulation*, in M. Bergström, V. Mitsilegas, T. Quintel (eds.), "Research Handbook on EU Criminal Law", 2nd ed., Edward Elgar, 2024

V. Franssen (2018), *The European Commission's E-evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement?*, in "European Law Blog. News and Comments on EU Law", 2018

G. González Fuster, S. Vázquez Maymir (2020), *Cross-border Access to E-Evidence: Framing the Evidence*, Center for European Policy Studies (CEPS), 2020

A. Juszczak, E. Sason (2023), *The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice An Introduction to the New EU Package on E-evidence*, in "Eucrim: the European Criminal Law Associations' forum", 2023, n. 2

K. Lenaerts (2017), *La vie après l'avis: exploring the principle of mutual (yet not blind) trust*, in "Common Market Law Review", vol. 54, 2017, n. 3

T. Marguery (2016), *Rebuttal of Mutual Trust and Mutual Recognition in Criminal Matters: Is 'Exceptional' Enough?*, in "European Papers", vol. 1, 2016, n. 3

V. Mitsilegas (2020), *Trust*, in "German Law Journal", Special Issue 1: "20 Challenges in the EU in 2020", vol. 21, 2020

V. Mitsilegas, (2019), *The European Model of Judicial Cooperation in Criminal Matters: Towards Effectiveness based on Earned Trust*, in "Revista Brasileira de Direito Processual Penal", vol. 5, 2019, n. 2

V. Mitsilegas, (2018), *The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence*, in "Maastricht Journal of European and Comparative Law", vol. 25, 2018, n. 3

V. Mitsilegas, (2014), *Transatlantic counterterrorism cooperation and European values: The elusive quest for coherence*, in E. Fahey, D. Curtin (eds.), "A Transatlantic Community of Law: Legal Perspectives on the Relationship between the EU and US Legal Orders", Cambridge University Press, 2014

A. Mosna (2024), *Judicial Protection in EU Cross-Border Evidence-Gathering: the EIO as a Case Study*, in "EuCLR European Criminal Law Review", vol. 14, 2024, n. 2

E.A. Ontanu (2023), *The digitalisation of European Union procedures: A new impetus following a time of prolonged crisis*, in "Law, Technology and Humans", vol. 5, 2023, n. 1

E.A. Ontanu (2022), *Normalising the use of electronic evidence: Bringing technology use into a familiar normative path in civil procedure*, in "Oñati Socio-Legal Series", vol. 12, 2022, n. 3

K. Propp (2024), *Navigating Toward an EU-U.S. Agreement on Electronic Evidence*, in"Lawfare", 1 December 2023

A. Sachoulidou (2024), *Cross-border access to electronic evidence in criminal matters: The new EU legislation and the consolidation of a paradigm shift in the area of 'judicial' cooperation*, in "New Journal of European Criminal Law", vol. 15, 2024, n. 3

J. Sarkowicz (2022), *Legal representative in the proceedings of gathering e-evidence under European Production Order: de lege lata remarks and de lege ferenda postulates*, in "EuCLR European Criminal Law Review", vol. 12, 2022, n. 1

T. Schauenburg, D. Zapf, N. Rossbrey, F. Málaga (2023), *EU breaks down digital borders: New e-Evidence rules facilitate cross-border investigations*, in "White & Case", 2023

R. Sicurella (2018), *Fostering a European criminal law culture: In trust we trust*, in "New Journal of European Criminal Law", vol. 9, 2018, n. 3

S. Signorato (2023), *Cross-Border Gathering of E-Evidence: Different Legal Frameworks in European Union and Council of Europe*, in "Journal of Eastern European Criminal Law", 2023, n. 1

B. Sippel (2023), *Guest Editorial*, in "Eucrim: the European Criminal Law Associations' forum", 2023, n. 2

S. Stolton (2018), *Council makes half-hearted agreement on e-Evidence*, in "EURACTIV", 2018

I. Szijártó (2023), *The Interplay Between the European Investigation Order and the Principle of Mutual Recognition*, in "European Papers", vol. 8, 2023, n. 3

S. Tosza (2024), *Mutual recognition by private actors in criminal justice? E-evidence regulation and service providers as the new guardians of fundamental rights*, in "Common Market Law Review", vol. 61, 2024, n. 1

S. Tosza (2023), *The E-Evidence Package is Adopted: End of a Saga or Beginning of a New One?*, in "European Data Protection Law Review", vol. 9, 2023, n. 2

S. Tosza (2021), *Internet service providers as law enforcers and adjudicators. A public role of private actors*, in "Computer law & Security review", vol. 43, 2021

M. Velicogna (2018), *e-Justice in Europe: From National Experiences to EU Cross-Border Service Provision*, in L. Alcaide Muñoz, M.P. Rodríguez Bolívar (eds.) "International e-Government Development. Policy, Implementation and Best Practices"w, Palgrave Macmillan, 2018

M. Velicogna (2014), *Coming to Terms with Complexity Overload in Transborder e-Justice: The e-CODEX Platform,* in F. Contini, G.F. Lanzara (eds.), "The Circulation of Agency in E-Justice", Springer, 2014

M. Velicogna, E. Steigenga, S. Taal, A. Schmidt (2020), *Connecting EU Jurisdictions: Exploring How to Open Justice Across Member States through ICT*, in "Social Science Computer Review", vol. 38, 2020, n. 3

T. Wahl (2023), *E-evidence Regulation and Directive Published*, in "Eucrim: the European Criminal Law Associations' forum", 2023, n. 2