BRIEFING

EU Legislation in Progress

European Parliament

Electronic evidence in criminal matters

OVERVIEW

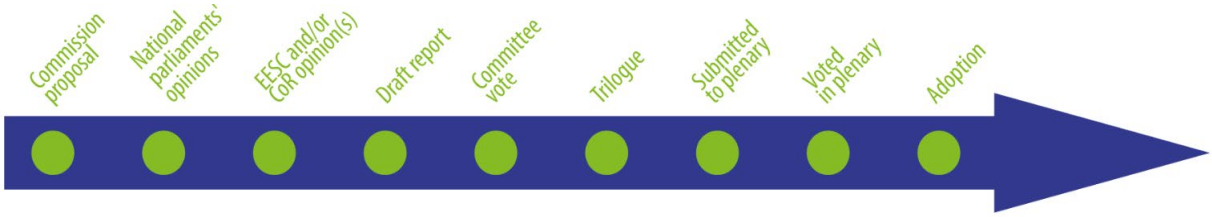
In June 2023, the European Parliament and the Council of the EU adopted two legal acts – a regulation and a directive – on electronic evidence in criminal matters. In the course of the legislative procedure, the two acts drew broad, often critical comments from data protection bodies, civil society and industry stakeholders.

The new rules will allow law enforcement and judicial authorities to directly request (or temporarily secure) electronic data needed for investigating and prosecuting crime from electronic service providers operating in the EU (wherever the data is stored). Moreover, they will impose an obligation on these service providers to appoint a legal representative for the purpose of gathering evidence and answering competent authorities' requests. The two legal acts are part of a broader array of international efforts to improve the legal framework and address persistent legal uncertainty that affects law enforcement and private parties alike.

A: Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters

B: 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

Committee responsible:	Civil Liberties, Justice and Home Affairs (LIBE)	A: COM(2018) 225 17.4.2018 2018/0108(COD)
Rapporteur:	Birgit Sippel (S&D, Germany)	
Shadow rapporteurs:	Nuno Melo (EPP, Portugal) Moritz Körner (Renew Europe, Germany) Sergey Lagodinsky (Greens/EFA, Germany) Patryk Jaki (ECR, Poland) Annalisa Tardino (ID, Italy) Cornelia Ernst (The Left, Germany)	B: COM(2018) 226 17.4.2018 2018/0107(COD)
Procedure completed.	Regulation (EU) 2023/1543 Directive (EU) 2023/1544 OJ L 191, 28.7.2023, pp 118-190	Ordinary legislative procedure (COD) (Parliament and Council on equal footing – formerly 'co-decision')



EPRS | European Parliamentary Research Service

Author: Piotr Bąkowski
Members' Research Service

PE 690.522 – September 2023

EN

Introduction

Electronic evidence can be defined as any data that can serve as evidence, regardless of whether it is stored on or generated, processed or transmitted by an electronic device. It includes both 'content data', such as e-mails, text messages and photographs, and 'non-content data', such as subscriber and traffic data (e.g. the routing or timing of a message). Such data are held by a variety of service providers, including providers of electronic communications and internet services. Whilst criminal investigations (both cross-border and domestic) tend to rely increasingly on this form of evidence,[1] law enforcement and judicial authorities often encounter difficulties in accessing it.

The volatility of electronic data is one such difficulty, as they can easily be deleted, altered or transferred. The data minimisation principle requires data to be adequate, relevant and limited to what is necessary for a specified purpose: they should only be retained as long as they are needed to fulfil that purpose. With this principle in mind, especially in the absence of mandatory retention prescribed by law, service providers tend to delete the data in their possession as quickly as possible, to the detriment of public authorities collecting evidence in the context of criminal investigations or proceedings.

The advancement of the internet, including the emergence of cloud computing, has brought on yet another set of difficulties, adding a layer of complexity to the thorny issue of jurisdictional interaction. Many service providers have their corporate seats or store data outside the country of investigation (notably in the United States (US) and Ireland). On some occasions, it is even difficult to determine where the data are located; on others, they may be split between countries, raising questions about the applicable national law.

Existing situation

The legal framework regarding cross-border access to evidence is characterised by the coexistence of multiple levels of regulation, such as international conventions and bilateral agreements, EU law pertaining to judicial cooperation in criminal matters but also to data protection, and a whole range of national laws. With the largest service providers being based in the US, developments in their legislation and jurisprudence also merit close attention.

The standard formal procedure for obtaining evidence located in one country to be used for criminal investigation or proceedings in another country is laid down in international conventions providing for mutual legal assistance (MLA), a traditional form of cross-border cooperation between public authorities. These include the Council of Europe European Convention on Mutual Assistance in Criminal Matters, the United Nations Convention on Transnational Organized Crime and the Council of Europe Convention on Cybercrime (the Budapest Convention), dealing specifically with electronic evidence. The latter has been ratified not only by most EU Member States (except for Ireland and Sweden) but also by several non-European countries, including the US. The EU is an observer organisation to the Council of Europe's Cybercrime Convention Committee.

Individual EU Member States have also signed various MLA treaties with third countries. Moreover, the EU has entered into several framework agreements, most importantly with the US, which is the main recipient of MLA requests for electronic evidence from EU Member States.

The MLA mechanism was designed before the internet era and has hence been considered by some as inadequate to secure evidence in the form of extremely volatile electronic data. Moreover, the number of requests – costly in terms of the resources involved – has grown exponentially and so has the time needed to answer them. In 2018, the Commission estimated that there were around 13 000 requests on e-evidence between EU Member States per year and approximately 1 300 requests from EU to US public authorities. It took US authorities 10 months on average to answer a single such request.[2] Even the very idea of using the MLA mechanism for cases involving electronic evidence could be called into question: it is meant to protect the sovereignty of the requested state, which in fact may not be at stake in most situations involving electronic evidence, there often being no connection between the offence and the country where the data are stored.

In the EU, the MLA mechanism has been gradually replaced with mutual recognition instruments. The European Investigation Order (EIO), introduced by Directive 2014/41/EU, is the mutual recognition tool used for cross-border requests related to all types of evidence. The directive does not apply to Denmark nor, quite importantly, to Ireland, where many service providers are based. The EIO is a decision issued or validated by a judicial authority in one Member State, for an investigative measure to be carried out by a similar authority in another Member State. It may also be used to obtain already existing evidence. The EIO has facilitated the cross-border exchange of evidence within the EU: judicial authorities communicate directly with one another without the mediation of any central authorities (as required under the MLA mechanism) and there are few admissible grounds for refusal. The procedure is also faster: the executing authority has 30 days to decide whether to execute the order and 90 days to carry out the requested measure; deadlines can be shortened in urgent circumstances. Moreover, the EIO may call for provisional measures, to be decided on by the executing authority within 24 hours, in order to prevent, e.g. the destruction or transformation of an item. The EIO may furthermore be used to preserve electronic data. However, one could argue that even though the EIO procedures are faster and less cumbersome than the MLA procedures, the exchange of electronic evidence would require even more expeditious channels.

The above challenges linked to the formal processes have led to the creation of an alternative channel of cooperation, with authorities making direct requests to service providers, including those in the US. Whereas US law does not regulate how service providers should respond to such direct requests, the US Department of Justice (DOJ) has encouraged them to respond favourably. However, this practice only concerns non-content data and US service providers have developed their own policies as to whether and how to respond. Such voluntary cooperation may result in unequal treatment of the requesting authorities across the EU. Overall, according to the European Commission, fewer than half of all the requests made to service providers outside the EU through both formal channels and direct cooperation are fulfilled.[3]

Some EU Member States have addressed the above limitations by making it obligatory for service providers to answer data requests ('production orders') by the authorities in charge of criminal investigations and proceedings, regardless of where the data are stored. Any state claiming jurisdiction for introducing such an obligation does so based on a 'connecting factor' (an element linking the data with its legal system). In the past, the use of connecting factors other than that of data location was widely believed to violate the territorial sovereignty of the state in which the data were located. There is a tendency, however, to expand the catalogue of acceptable connecting factors that may now also include the place where the service provider is established or offers its services.[4] Such divergent national approaches result in legal uncertainty for all actors involved: public authorities face potential conflicts of jurisdiction, service providers risk being under conflicting obligations and incurring sanctions, and there is no clarity for users as to the state competent to access their data.

Access of law enforcement to data raises questions regarding compliance with the rights to privacy and to protection of personal data enshrined in EU law, notably in the Charter of Fundamental Rights of the EU (the EU Charter) and in secondary law instruments such as the General Data Protection Regulation (GDPR), the Data Protection Law Enforcement Directive and the e-Privacy Directive. In this regard, the annulment of the 2006 Data Retention Directive by the Court of Justice of the EU (CJEU) has had a serious impact on law enforcement's ability to collect evidence: in its *Digital Rights Ireland* and *Tele2* rulings, the CJEU held that general and indiscriminate retention of traffic and location data entailed a particularly serious interference with privacy and data protection rights.[5] Revoking the Data Retention Directive resulted in a patchwork of national laws, with most Member States still providing for retention obligations (though for varying periods of time), but some not having a data retention regime in place.

Comparative elements

The new rules need to be read in the context of international and US laws, notably the Budapest Convention and the provisions of the US CLOUD Act of 2018.

The Budapest Convention is the most relevant element of the international framework for both domestic and cross-border access to electronic evidence. Its provisions on MLA take into account the urgency of the requests for the release of electronic evidence, providing for possibilities to accelerate the proceedings, including through expedited means of communication (e.g. fax or e-mail) and the requirement to designate points of contact available 24/7. Moreover, the convention allows ordering the expeditious preservation of data.

The convention grants national authorities the possibility of ordering the disclosure of (specific types of) data by service providers: under Article 18(1)(b) of the convention, a production order can be issued to any service provider offering its services in a state party's territory to submit subscriber information relating to such services, which is in their possession or control. At the same time, each person in the state party's territory can be ordered to submit specified computer data in their possession or control, stored in a computer system or a computer-data storage medium (Article 18(1)(a)). The interpretation of these two provisions is subject to debate.[6]

In January 2023, the Parliament voted to move forward with ratifying the Second Additional Protocol to the convention devoted specifically to enhanced international cooperation regarding electronic evidence. The aim is to improve both the MLA procedures and direct cooperation with service providers in other jurisdictions, while also providing stronger safeguards, notably regarding data protection.

While the US is party to the convention, in 2018 it adopted the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), stirring controversy regarding this new act's impact on foreign jurisdictions. The CLOUD Act amended the 1986 Stored Communications Act as a consequence of a legal dispute, which involved Microsoft and culminated in a US Supreme Court case regarding the possibility for US federal law enforcement to order US-based companies to provide data stored abroad. It resulted in no judgment as the passage of the Cloud Act rendered it unnecessary.

Under the CLOUD Act, service providers having their seat in the US are obliged to comply with US orders to disclose content data, regardless of where they are stored. Moreover, the act provides for a possibility for the US to enter into 'executive agreements' with foreign jurisdictions. On the basis of such agreements, US and foreign public authorities investigating serious crime could make direct requests to service providers in the other jurisdiction to deliver specific content data (as explained above, at present, US service providers disclose only non-content data and do so on a voluntary basis). The agreements cannot cover the data of US persons, i.e. citizens, permanent residents and companies incorporated in the US. Service providers can challenge the order if there is a risk of it violating their national law.

The CLOUD Act has been criticised for unilaterally imposing an obligation on all entities having their seat in the US to disclose data located outside the US, which, some argue, amounts to US law having extraterritorial effect and is likely to lead to conflicts of law. Orders issued under the CLOUD Act may arguably be incompatible with the GDPR, which provides for a very restrictive set of criteria to be met with respect to the lawful transfer of an EU citizen's personal data to any third country. Service providers violating the GDPR risk incurring administrative fines of up to €20 million or up to 4 % of their worldwide annual revenue.

To address the conflict of law and data protection issues while allowing for the transfer of evidence on a reciprocal basis through direct orders issued to service providers, the Commission is currently negotiating a framework agreement on cross-border access to electronic evidence with the US. The negotiations started in 2019, stalled to give the co-legislators time to finalise their work on the e-evidence package, and then resumed in March 2023.

Parliament's starting position

In its resolution of October 2017 on the fight against cybercrime, the European Parliament underlined that a common EU approach to criminal justice in cyberspace was a matter of priority, as it would improve the enforcement of the rule of law in cyberspace and facilitate the obtaining of

e-evidence in criminal proceedings. The Parliament called on the Commission to put forward an EU legal framework for e-evidence, including harmonised rules to determine the status of a provider as domestic or foreign, while stressing that any e-evidence framework should include sufficient safeguards for the rights and freedoms of all concerned and protect providers from requests that could create conflicts of law or otherwise impinge on the sovereignty of other states. In a December 2017 resolution on the implementation of the Child Sexual Abuse Directive, the Parliament pointed to the access to electronic evidence as one of the main challenges faced by law enforcement and judicial authorities in the investigation and prosecution of child sexual abuse offences committed online. In the findings and recommendations of its Special Committee on Terrorism, the Parliament also underlined the importance of electronic evidence for investigating terrorist offences.

Council & European Council starting position

At the end of 2015, the Justice and Home Affairs Council initiated a reflection process on effective criminal justice in the digital age, which continued into 2016, notably at the conference on jurisdiction in cyberspace organised by the Dutch Presidency of the Council. The initiative gained impetus after the Brussels terrorist attacks of March 2016, with a joint statement stressing the need to 'find ways, as a matter of priority, to secure and obtain more quickly and effectively electronic evidence, by intensifying cooperation with third countries and with service providers that are active on European territory'. In its June 2016 conclusions, the Council advocated the development of a common EU approach on improving criminal justice in cyberspace. Practical solutions to enhance the effective conduct of criminal proceedings in cyberspace would include enhancing cooperation with service providers, accelerating and streamlining MLA procedures and efficiently using mutual recognition procedures to secure and obtain e-evidence, while fully respecting data protection and fundamental rights frameworks. The Council asked the Commission to assess the possibilities for such a common approach, including a possible legislative initiative. The European Council also considered, in its June 2017 conclusions, that effective access to electronic evidence was essential to combating serious crime and terrorism. In October 2018, the EU Heads of State and Government called for the Commission proposals on e-evidence to be agreed on by the end of the legislature.

Preparation of the proposal

In its European agenda on security 2015-2020, the Commission committed to examine the obstacles standing in the way of criminal investigations on cybercrime, notably as regards issues of competent jurisdiction and rules on access to evidence and information. In the 2016 follow-up communication on an effective and genuine security union, the Commission clarified that rapidly securing and obtaining electronic evidence is a key element in successfully preventing, investigating and prosecuting not only cybercrime but also other serious crimes, in particular terrorism. It announced its intention to propose, by the summer of 2017, solutions to address the problems of obtaining electronic evidence in relation to criminal investigations, including in the form of legislation, if required. As a follow-up to the Council conclusions on improving criminal justice in cyberspace, the Commission presented a non-paper in December 2016 and conducted, between June 2016 and May 2017, an extensive expert consultation with a wide range of stakeholders (Member States' ministries, judiciary and law enforcement, industry, civil society, academia, EU agencies, etc.), leading to the publication of a second non-paper presenting the findings and charting a possible way forward. In August 2017, the Commission published its inception impact assessment and also launched an open public consultation. Both the consultation process and the surveys among public authorities and service providers, covering topics such as current practices, the scale of the problem and costs and benefits are detailed in the Commission's impact assessment (IA). For more information, see the EPRS initial appraisal of the IA.

The changes the proposals would bring

As stated by the Commission, the two legislative proposals sought to adapt cooperation mechanisms to the digital age, by providing the judiciary and law enforcement with adequate tools to counter modern forms of criminality. The proposed regulation on European production and preservation orders was intended to allow the competent authorities of one Member State to request directly from a service provider established or represented in another Member State access to, or preservation of, electronic data needed for the investigation and prosecution of crimes covered by the regulation. As for the proposed directive, it sought to require from service providers operating in one or more Member States to designate at least one legal representative in the EU in charge of receiving and enforcing orders issued by competent authorities from across the EU.

Regulation on European production and preservation orders

Legal basis: The legal basis chosen for the regulation – the centrepiece of the proposed legislation – is Article 82(1) of the Treaty on the Functioning of the European Union (TFEU), providing for the possibility of adopting measures to facilitate cooperation between the Member States' judicial or equivalent authorities in relation to proceedings in criminal matters and the enforcement of decisions. According to the Commission, this legal basis is applicable to the proposed mechanisms of direct cooperation between judicial authorities and service providers, as 'Article 82(1) ensures mutual recognition of judicial decisions by which a judicial authority in the issuing State addresses a legal person in another Member State and even imposes obligations on it, without prior intervention of a judicial authority in that other Member State'. As the Commission itself recognises in its IA, 'this would introduce a new dimension in mutual recognition, beyond the traditional judicial cooperation in the Union, so far based on procedures involving two judicial authorities, one in the issuing State and another in the executing State' – a major change, which is not uncontroversial.

Objective: The proposed regulation introduced two new investigative measures: 1) the European production order for requesting the production of data stored by a service provider located in another jurisdiction within 10 days of receipt of the order (6 hours in emergency cases); and 2) the European preservation order for requesting the preservation of such data so as to prevent their removal, deletion or alteration, for a period of 60 days, in view of a subsequent request for the production of this data through MLA channels (in case of third countries), an EIO (between participating Member States) or a European production order. The two kinds of orders would be transmitted to the addressee through a European Production Order Certificate (EPOC) and a European Preservation Order Certificate (EPOC-PR) respectively.

Scope: Both types of orders refer to the specific known or unknown perpetrators of a criminal offence that has already taken place and only allow the production or preservation of data that had already been stored at the time of receipt of the order. The Commission made it clear that the proposal did not introduce any general data retention obligations and did not cover real-time interception of telecommunications. The orders should be necessary and proportionate and could be used only in criminal proceedings, from the initial pre-trial investigative phase until the closure of the proceedings by judgment or another decision. The proposal envisaged some differentiation based on the types of data concerned (see 'Data categories' below) and their level of interference with fundamental rights. First, orders for producing subscriber and access data could be issued for any criminal offence, whilst orders for producing transactional or content data may only be issued for criminal offences punishable in the issuing state by a maximum custodial sentence of at least three years, or for specific crimes (fraud and counterfeiting of non-cash means of payment, child sexual abuse, cybercrime and terrorism). Second, the rules envisaged that both types of orders need to be issued or validated by a judicial authority of a Member State; however, orders for producing transactional and content data had to be issued by a judge or court, whilst orders for subscriber or access data could be issued by a prosecutor as well. As for preservation orders, these may be issued for all criminal offences and all data categories, by a judge or a prosecutor. The regulation would

apply to all service providers that offer services in the EU, wherever their headquarters are located or information stored.

Data categories: The proposed regulation classified data into four categories according to their level of intrusiveness: subscriber data, access data, transactional data (the three categories referred to jointly as 'non-content data') and stored content data. This categorisation differs from the approach used in existing EU and international instruments, such as the Budapest Convention,[7] with the notable addition by the Commission of the new category of 'access data'. The Commission proposed the following definitions:

- **subscriber data**: any data pertaining to: a) the identity of a subscriber or customer such as the provided name, date of birth, postal or geographical address, billing and payment data, telephone, or email; b) the type of service and its duration;
- **access data:** data related to the commencement and termination of a user access session to a service, which are strictly necessary for the sole purpose of identifying the user of the service (date and time of use, log-in to and log-off from the service, IP address, user ID);
- **transactional data**: data related to the provision of a service offered by a service provider that serve to provide context or additional information about such service and are generated or processed by an information system of the service provider (e.g. metadata, location data);
- **content data**: any stored data in a digital format such as text, voice, videos, images, and sound other than subscriber, access or transactional data.

All categories contain personal data and are thus covered by the EU data protection *acquis*.

Safeguards and remedies: Besides the applicable data protection rules and procedural criminal law provisions, the proposal provided for safeguards for persons whose data are being sought, such as the possibility to challenge the legality, necessity and proportionality of the order. The individuals affected could exercise their right to effective remedy only in the issuing Member State. The issuing Member State also has to take into account any immunities and privileges that protect the data sought in the Member State of the service provider. Service providers would be able to oppose the received order on defined grounds, such as technical issues, de facto impossibility or orders that are manifestly abusive or in violation of the EU Charter. In addition, a specific review procedure (by a competent court in the issuing Member State) would be set up for situations where the obligation to provide data conflicts with a competing obligation arising from the law of a third country. The procedure differs depending on the grounds prohibiting the disclosure of data: should there be any conflicting obligations based on fundamental rights/interests of the third country (e.g. national security), this requires the involvement of its central authority (Article 15 of the proposal).

Costs and sanctions: Service providers may claim reimbursement of their costs by the issuing State, if this is provided for in its national law for domestic orders in similar situations. On the other hand, Member States should lay down effective and proportionate pecuniary sanctions applicable to infringements by service providers of their obligations regarding the execution of the orders.

Directive on the appointment of legal representatives

The proposal for a directive was exclusively based on internal market provisions: Articles 53 TFEU (freedom of establishment of self-employed persons) and 62 TFEU (freedom to provide services). The directive would impose on both European service providers operating in more than one Member State and non-European service providers offering services on the EU market the obligation to appoint a legal representative in (at least) one Member State. The appointed legal representative would function as a single contact point for national competent authorities. Service providers should notify the appointment to the central authority of the host Member State, in charge of ensuring compliance with the future orders addressed to the legal representative by the other Member States' authorities. Sanctions were also to be in place in case of non-compliance.

Advisory committees

In its opinion of 12 July 2018, the European Economic and Social Committee (EESC) welcomed the proposals, in particular the fact that the regulation would introduce binding European instruments for securing and accessing data, but also underlined the importance of respecting fundamental rights. The EESC supported the development of EU-wide uniform standards regarding the conditions for access to data; however, it found it problematic that a production order for subscriber and access data could also be issued by a prosecutor and advocated extending scrutiny by a judge to the gathering of all personal data. It also considered that the objective of ensuring that European Production Orders for transactional and content data are used only for more serious crimes would be better achieved by applying a minimum three-month penalty (to serve as a guideline), rather than a maximum three-year penalty. As for the proposed directive, the EESC welcomed the mandatory appointment of legal representatives by all service providers operating in the EU, as a move that would bring more clarity both for judicial authorities and for providers themselves. It advocated the service providers' right to reimbursement of costs in all cases where this is provided for in the law of the issuing State.

National parliaments

No reasoned opinions had been submitted by the deadlines set for the subsidiarity checks: 13 September 2018 for the regulation and 10 September 2018 for the directive. The Czech Senate, the German Bundesrat, the Portuguese Parliament and the Spanish Congress of Deputies entered into political dialogues with the Commission. The German Bundestag expressed concerns as regards the legal basis for the regulation, assuming that direct taking of evidence in another Member State can hardly be subsumed under mutual recognition. Both the German Bundesrat and the Czech Senate raised concerns about the safeguards for fundamental rights standards in the regulation and about the high administrative costs the regulation would entail, specifying that the additional burden for service providers should be as low as possible. The Czech Senate also advocated for an extension of the preservation period of the data requested by the EPOC-PR to 90 days (instead of 60), for the postponement of the entry into force of the regulation, and for a prolongation of the transposition period of the directive to 24 months.

Stakeholder views

Data protection bodies reminded that law enforcement's access to personal data constitutes an interference with the rights to privacy and data protection, guaranteed respectively under Articles 7 and 8 of the EU Charter, and that limitations may be imposed on the exercise of these rights and freedoms only if they are necessary and if they genuinely meet the objectives of general interest recognised by the EU, or the need to protect the rights and freedoms of others. Both the Article 29 Working Party and its successor, the European Data Protection Board (EDPB), called for ensuring the proposals' consistency with EU data protection law and for taking into account the relevant case law at EU level. The EDPB also advised restricting the scope of the proposed regulation to data controllers in the sense of the GDPR (or otherwise including an obligation to inform the controller).

In its opinion, the European Data Protection Supervisor (EDPS) underlined the need for greater involvement of the judicial authorities in the enforcing Member State and for clarifying the definitions of data categories in the regulation, advising a reassessment of the balance between the types of offences for which EPOCs could be issued and the categories of data concerned. The EDPS identified several aspects requiring improvement: the authenticity and confidentiality of orders and data transmitted; the limited preservation under the EPOC-PRs; the applicable data protection framework; the rights of data subjects; the data subjects benefiting from immunities and privileges; the legal representative; the time limits for complying with EPOCs; and the possibility for service providers to object to orders. The EDPS asked for more clarity on how the regulation would interact with future international agreements, underlining that maintaining a high level of data protection

in the EU should become a standard requirement when negotiating international agreements on cross-border access to electronic evidence.

Internet service providers (ISPs) and other industry representatives voiced multiple concerns in relation to the proposed e-evidence regime. EuroISPA, a pan-European association of ISPs, strongly advocated for ISPs not to become those responsible for checking orders against the national laws and assessing compliance with the EU Charter, criticising 'further privatisation of law enforcement'. It called for exemptions to be granted to small and medium-sized enterprises to offset the considerable administrative, legal and financial burden. Moreover, EuroISPA advocated harmonising data categories across EU legislation to provide legal certainty and facilitate compliance.

EuroISPA, together with other associations representing users, European and international companies, and legal practitioners, signed a joint statement urging EU legislators to 'strike the right balance between expanding law enforcement's ability to gather electronic evidence and protecting fundamental rights in the new e-Evidence legislation'. In February 2021, the BSA, representing the software industry, published a position paper making several recommendations for the final version of the proposed regulation, building on the amendments put forward by the Parliament.

From the **digital industry** side, Microsoft and DIGITALEUROPE expressed reservations regarding the general approach agreed by the Council in December 2018, as missing some principal safeguards. Microsoft called on EU legislators to: 1) establish notice-by-default for persons targeted by orders issued under the proposed regulation; 2) require a means to ensure EU Member States can invoke protection for their citizens and the organisations located on their territory; 3) give service providers the right to contest an order when they believe the demand is unlawful, overbroad, or otherwise inappropriate; 4) and to require law enforcement agencies to use EPOs or other EU measures, rather than domestic procedures, for cross-border scenarios. A whole range of **civil society organisations**, among them European Digital Rights (EDRi), the Meijers Committee, and the Council of Bars and Law Societies of Europe (CBBE), have expressed their views at various stages of the legislative procedure, commenting on the potential negative effects of the proposals. The recurrent issues of concern raised include the choice of Article 82 TFEU as the legal basis for the proposed regulation, inadequate remedies for affected persons, insufficient involvement of judicial authorities in the enforcing Member State, as well as the lack of added value of the proposals, considering the EIO and the MLA mechanisms already in place.

Following the political agreement on the two proposals, a coalition of 24 civil society groups, associations of media and journalists and of internet service providers and professional associations urged the co-legislators in an open letter to revise the compromise text of the proposed regulation, as it contained provisions that severely undermine fundamental rights, including press and media freedom, the rights of the defence, the right to privacy and medical patients' rights. The letter criticised extensively the notification procedure for its deficiencies an example being the fact that the proposal gives the authorities of the issuing Member State discretion to decide what the residence of the person whose data is sought, is (the residence affects the notification obligation). The letter also argued that mandatory notification should extend to subscriber data and traffic data sought for the sole purpose of identifying the person, given that in some cases this data may be sensitive (e.g. when it concerns whistle-blowers or journalistic sources). The coalition held the view that notification should always suspend the disclosure obligation of the service provider until the enforcing authority validates disclosure (the compromise text of the proposed regulation did not require such active validation). Furthermore, the coalition inquired about what would the consequences be if the enforcing authorities failed to raise grounds for refusal, in contravention of the requirement to do so.

In February 2023, EDRI commented on the compromise text, stressing that a robust notification system would require systematically sending the order to a judicial authority that would verify its legality and proportionality, before it is sent to the service provider. While praising the Parliament's

initial position, EDRI criticised the trilogues' outcome, elaborating on the notification-related arguments exposed in the open letter it had co-signed and pointing to weaknesses of the protection against fundamental rights' violations, in particular as regards people residing in Member States with systemic rule of law deficiencies.

Academic views

Two studies conducted in 2018 on the request of the LIBE committee, expressed reservations regarding the new instruments. In the first one, on criminal procedural laws across the EU, the authors raised doubts about the legal basis of the proposed e-evidence regulation, the role given to service providers in safeguarding fundamental rights, the limited judicial control and the disputable distinction between access data and transactional data in light of CJEU case law on the sensitivity of metadata. The second one – an assessment of the Commission proposals – identified some major shortcomings of the proposed regulation and voiced scepticism on whether it provides for effective remedies and creates more legal certainty, considering its significant reliance on national laws. Several other researchers expressed criticism, pointing to the 'privatisation of mutual trust' in the EU criminal justice area. In a 2020 study on cross-border data access in criminal proceedings, the Centre for European Policy Studies (CEPS) and the Queen Mary University of London task force recommended withdrawing the e-evidence proposals on account of their far-reaching negative implications for legal certainty and failure to demonstrate added value, necessity and proportionality. The task force suggested strengthening the existing EIO and creating a single EU portal for transmission of digital EIOs as a way to speed up and streamline the exchange of evidence.

Legislative process

The **Council** adopted its general approach on the proposed regulation on 7 December 2018, even though it did not reach full consensus among the Member States. It agreed its position on the proposed directive on 8 March 2019.

In its general approach, the Council introduced a number of changes to the proposed regulation. These: i) extended the latter's scope for criminal proceedings aimed at localising a convict that absconded from justice; ii) set the level of pecuniary sanctions that can be imposed on service providers in case of non-compliance (up to 2 % of total worldwide annual turnover of the preceding financial year); iii) and introduced a notification procedure to the enforcing Member State (only for production orders targeting content data). The enforcing State's authorities would be notified of an EPOC whenever the issuing authority believes that the person whose data are sought is not residing in the issuing authority's own territory; such a notification would not have a suspensive effect. It mainly aimed to give the enforcing State an opportunity to flag whether the data requested is protected by immunities and privileges, or is subject to rules on the determination and limitation of criminal liability related to freedom of expression, or whether the disclosure of this data may impact fundamental interests of the State. Another change the Council made is iv) to add the speciality principle that limits the use of electronic evidence only to the purpose of the proceedings for which it was obtained. On the other hand, it v) deleted the subsection on non-execution of orders being manifestly abusive or violating fundamental rights (Article 9(5)) and vi) abolished the specific review procedure involving the giving of an opinion by the authorities of a third country in case of a conflict of law based on fundamental rights or fundamental interests of that third country. The Council raised from 6 to 24 months the period after which the regulation would become applicable.

The Council's position on the proposed directive included changes to the Commission's initial proposal, such as provisions introducing: i) a clearer joint responsibility for service providers and legal representatives; ii) arrangements to limit the burden for SMEs, including the possibility for several service providers to appoint the same legal representative; and a transposition deadline of 18 months.

Within the **European Parliament**, the proposals were assigned to the LIBE committee (rapporteur: Birgit Sippel, S&D, Germany). The Internal Market and Consumer Protection Committee (IMCO) was

asked for an opinion but decided not to give one. No Parliament position was adopted during the 2014-2019 term. In October 2019, work in LIBE resumed, with Birgit Sippel reappointed as rapporteur. In her draft report presented in November 2019, she proposed a large number of changes to the proposed regulation and recommended integrating the relevant parts of the directive into it, instead of having a separate instrument. LIBE finally adopted its report on the proposed regulation on 7 December 2020, by 35 votes in favour, 22 against and 7 abstentions, together with the decision to open interinstitutional negotiations (55 votes in favour, 7 against and 2 abstentions). The negotiation mandate was confirmed in plenary on 16 December 2020.

In its position, the Parliament modified the data categories, abolishing the new category of 'access data', and sticking to more traditional categories of 'subscriber data', 'traffic data' and 'content data'. Parliament established a differentiation for the execution of an EPOC for 'subscriber data and IP addresses for the sole purpose of identifying a person', on one hand, and for traffic or content data, on the other hand. Parliament replaced the term 'electronic data' with 'electronic information' and introduced a provision on the admissibility of such electronic information in court proceedings. It reinforced the provisions on effective remedies and introduced an obligation to inform, by default, the persons whose data is being sought, with any exception to be justified by a judicial order. The deadline for transmitting data in emergency cases was extended to 16 hours. The Parliament agreed on the notification procedure to the authorities of the executing state,[8] extended to all types of data and both the EPOC and the EPOC-PR. It introduced the possibility for the executing authority to refuse production orders, based on specific grounds for non-recognition or non-execution listed in the regulation. While the notification would not have a suspensive effect for subscriber data and IP addresses, the executing authority would have up to 10 days (16 hours in emergency cases) to refuse an EPOC whenever traffic data and content data are concerned. Moreover, in cases where the issuing state is subject to the procedure on the rule of law (Article 7(1) or (2) of the Treaty on European Union (TEU), the service provider should transmit the requested data only after having obtained the explicit written consent of the executing state's authority. Parliament also added a provision on establishing a common European exchange system with secure channels for the transmission of the orders and of the requested data between the competent authorities and service providers. Parliament proposed fixing the deadline for the Member States to start applying the regulation at 18 months.

As to the proposed directive, the LIBE committee voted to reject the Commission proposal and to integrate, directly into the proposed regulation, the relevant provisions on the appointment of legal representatives within the EU.

On 29 November 2022, after eight political trilogue meetings, the co-legislators reached a political agreement on the most controversial elements of the two proposals. The compromise was endorsed by the Council and the LIBE committee in January 2023. The agreed texts were formally adopted by the Parliament (2018/0107(COD)) and 2018/0108(COD)) and the Council in June 2023 and published in the Official Journal in July 2023.

The regulation, as adopted, retains the categories of subscriber data, traffic data and content data. It provides for a mandatory deadline of 10 days for responding to a production order, with a possibility to reduce it to 8 hours in emergency cases. Moreover, it sets up a notification system for content data and traffic data, except for data requested for the sole purpose of identifying the user. Notification is not required if 'the issuing authority has reasonable grounds to believe' that the offence 'has been committed, is being committed or is likely to be committed in the issuing State and 'the person whose data are requested resides in the issuing State'.

The enforcing state's national authorities will have 10 days or, in emergency situations, 96 hours, to raise one of the grounds for refusal listed in the regulation. These include situations where the requested data are protected by immunities or privileges or covered by criminal liability rules related to freedom of expression, and where there are substantial grounds to believe that the execution of the order would entail a manifest breach of fundamental rights. If such grounds of refusal are raised,

the service provider will have to stop the execution of the order and refrain from transferring the data and the issuing authority will have to withdraw the order. Moreover, the right to effective remedies has been included in the regulation to be exercised before a court in the issuing state under its national law. The Parliament report's provisions on expressed written consent for transfers to Member States covered by the procedure under Article 7 TEU were not retained in the final text.

Despite the Parliament's original objection, the Parliament and the Council adopted the directive using Articles 53 and 62 TFEU as its legal basis.

The directive must be transposed by 18 February 2026 and the regulation will become applicable on 18 August 2026.

EP SUPPORTING ANALYSES

Tuominen M., European production and preservation orders and the appointment of legal representatives for gathering electronic evidence, Initial Appraisal of a Commission Impact Assessment, EPRS, European Parliament, 2018.

Böse M., An assessment of the Commission's proposals on electronic evidence, study, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, 2018.

ENDNOTES

1 According to the Commission, e-evidence is relevant in around 85 % of all criminal investigations, and in almost two thirds (65 %) of the investigations where it is relevant, a request to service providers across borders (based in another jurisdiction) is needed. See Commission Impact Assessment, SWD(2018) 118 final, p. 13; see also Sirius EU Digital Evidence Situation Report - 2nd Annual Report, Europol, December 2020.

2 Commission Impact Assessment, pp 13-14 and p. 25.

3 Commission Impact Assessment, pp 15-16.

4 An assessment of the Commission's proposals on electronic evidence, European Parliament, 2018, pp 31-33.

5 As litigation cases on data retention continue, the CJEU judgements from October 2020 confirmed the established case law, yet introducing some exceptions (see comments by Juraj Sajfert on the European Law blog).

6 Critiquing DOJ's claim that the Budapest Convention requires the CLOUD Act's solution, E. Kyriakides, CBDF, posted on 9 July 2019; An assessment of the Commission's proposals on electronic evidence, op. cit., p. 13.

7 The convention distinguishes between subscriber information, traffic data and content data. See also Warken, C., et al. Re-thinking the categorisation of data in the context of law enforcement cross-border access to evidence, 2020.

8 The EP replaced the term 'enforcing State' by 'executing State', defined as the Member State in which the service provider is established or legally represented and to which the orders are transmitted for notification and enforcement. However, the Parliament's amendment was not retained in the final texts.

DISCLAIMER AND COPYRIGHT

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)

Second edition of a briefing originally drafted by Piotr Bąkowski and Sofija Voronova. The 'EU Legislation in Progress' briefings are updated at key stages throughout the legislative procedure.