The Proposal on Electronic Evidence in the European Union

Ángel Tinoco-Pastrana *

ABSTRACT

This article examines the origin, foundations and main features of the proposal of the European Union to facilitate cross-border access to electronic evidence, which was presented by the European Commission in April 2018. The creation of advanced solutions for the transnational gathering of electronic evidence in the EU is a very current and important issue, and is complemented with other actions carried out at an international level. Respect for the principle of proportionality must be particularly relevant in order to achieve the proper functioning of the new scheme. The main idea is that certificates of judicial orders will be transmitted directly to the legal representatives of online service providers. These new instruments of judicial cooperation (consisting of a Regulation and a Directive) aim at facilitating and accelerating judicial authorities' access to data in criminal investigations in order to assist in the fight against crime and terrorism. They should reduce response times in comparison to the instruments currently in place; service providers will be obliged to respond within ten days or, in urgent cases, within six hours. The proposal comes in reaction to the acute need to provide authorities with cutting-edge instruments for obtaining cross-border access to data.

AUTHOR

Ángel Tinoco-Pastrana

Profesor Titular de Derecho Procesal - Associate Professor of Procedural Law
Universidad de Sevilla

CITE THIS ARTICLE

Tinoco-Pastrana, Á. (2020). The Proposal on Electronic Evidence in the European Union. Eucrim - The European Criminal Law Associations' Forum. https://doi.org/10.30709/eucrim-2020-004

Published in eucrim 2020, Vol. 15(1) pp 46 – 50

https://eucrim.eu

ISSN:

I. Introduction – Setting the Scene

The creation of an instrument for transnational access to electronic evidence in the EU is a pressing issue, given its relevance to the fight against terrorism, cybercrime, and transnational crime in its entirety. The Area of Freedom, Security and Justice (AFSJ) needs to be able to vigorously respond to these forms of crime; establishing security is one of top policy priorities of the EU and it is closely linked to the European Research Area, in which security concerns are of paramount importance.[1]

In April 2018, the European Commission proposed new rules enabling police and judicial authorities to obtain electronic evidence more quickly and more easily. They were included in 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" and the accompanying "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."[2]

The fight against terrorism is the fundamental issue that drove the proposal. The background of the proposal dates back to the year 2016 and the terrorist attacks in Brussels of 22 March 2016. The "Joint Declaration of EU Ministers for Justice and Home Affairs Ministers and Representatives of EU Institutions" two days after the attacks stressed the need to "find ways, as a matter of priority, to secure and obtain more quickly and effectively digital evidence, by intensifying cooperation with … service providers that are active on European territory, in order to enhance compliance with EU and Member States' legislation and direct contacts with law enforcement authorities." It was further announced that the Council meeting in June 2016 would identify concrete measures to address this complex matter.[3] Subsequently, on 9 June 2016, the Justice and Home Affairs Council adopted the "Conclusions on the improvement of criminal justice in cyberspace and on the European Judicial Network on Cybercrime," which expressly highlighted the increased importance of electronic evidence in criminal proceedings, especially with regard to terrorism.[4] The European Council further pushed for adoption of EU legislation on e-evidence. At its meeting of 23 June 2017,[5] the Council emphasized that cross-border access to electronic evidence was deemed fundamentally important in the fight against terrorism. On 20 November 2017, the European Council asked the Commission to make a legislative proposal in early 2018.[6]

When issuing the legislative proposal on 17 April 2018, the European Commission stressed the growing importance of electronic evidence for criminal proceedings, the fact that cross-border requests for such evidence currently predominate in criminal investigations, and that criminals and terrorists cannot be allowed to exploit modern communication technologies to conceal their activities and evade justice. It was also highlighted that the authorities continue to work with complicated methods and that, although judicial cooperation and mutual assistance are necessary, the process is currently too slow and complex, enabling criminals to resort to state-of-the-art technologies. Authorities need to be equipped with 21st century techniques, given that approximately two thirds of electronic evidence is located in another State (both within and outside the EU), a fact that hinders both the investigation and the prosecution.[7]

The EU is not the only actor striving for new legislative measures in the area of electronic evidence. Terrorism is a global phenomenon, and access to electronic evidence also takes on a global dimension; therefore, the measures are not limited to the European level. The conventional judicial cooperation is important in the relationship with third States, mainly with the USA, where a great part of the electronic data is circulated and/or stored. At the June 2018 Justice and Home Affairs Council, the issue of transnational access to electronic evidence was once again addressed. Consensus was reached on continuing contacts and negotiations with the USA,[8] given the enactment of the CLOUD Act.[9] On 6 June 2019, the Council gave

https://doi.org/10.30709/eucrim-2020-004

two mandates to the Commission for the negotiation of international agreements on electronic evidence, which incorporated relevant guarantees as regards privacy and procedural rights: (1) a mandate to negotiate an agreement with the US to facilitate access to electronic evidence, taking into consideration conflicts of law and common rules for the direct and reciprocal transfer of evidence, and (2) a mandate to enter into negotiations with the Council of Europe on a second Additional Protocol to the Budapest Convention on Cybercrime.[10] The connection between these international developments and the EU proposal on e-evidence builds on the fact that these measures pursue facilitating access to electronic evidence when the evidence circulates or is stored outside the EU. The aim of the aforementioned agreements is to simplify and grant greater effectiveness to the mutual legal assistance regime by reducing the deadlines for access to electronic evidence and allowing for direct cooperation with service providers. The Council highlights the need for these agreements to coexist with the Regulation and the Directive on electronic evidence currently being processed in the EU.[11] Therefore, the agreements being negotiated by the European Commission would additionally boost a more homogeneous international regulation in this area.

The following two sections focus on an analysis of the proposed European Production and Preservation Orders. This includes a description of their main features, the legislative technique being used for the establishment of the new orders, and the most relevant recent aspects that the plans entail in the field of judicial cooperation (II.). Furthermore, the importance of the principle of proportionality is highlighted, both as regards the EU instrument as well as the instruments discussed at the international level (III.). It will be stressed that application of the proportionality principle will lead to a major improvement in this specific field of judicial cooperation.

II. The European Production Order and the European Preservation Order

The European production order (EPdO) and the European preservation order (EPsO) allow the judicial authority of a Member State, the issuing State, to directly order a provider offering the service in the EU to hand over or store the electronic evidence. The EPdO implies an extraordinary simplification of the procedure, with a significant reduction in deadlines for delivery of the evidence, i.e., ten days or – in emergency situations – six hours (Art. 9(1) and (2) of the text in the version of the Council's general approach,[12] which will be taken as a reference in this article). This considerably accelerates the obtainment of information compared to 120 days for the European Investigation Order (EIO) and 10 months in the area of (conventional) mutual legal assistance.[13]

These orders will be governed by an EU Regulation, which underscores that the EU is not willing to let effective use of these instruments be hampered by late transposition or even non-transposition on the part of the Member States – risks that exist within the scope of EU Directives, as recently happened with Directive 2014/41/EU on the European Investigation Order. The EU is setting a clear direction, as this legislative technique was also instrumental in Regulation (EU) 2018/1805 on freezing and confiscation orders and in the creation of the European Public Prosecutor's Office through Regulation (EU) 2017/1939. For the appointment of the legal representatives of service providers, however, who are essential for the execution of orders, a Directive with an 18-month transposition deadline has been chosen.[14] This could be an obstacle, since legal representatives play a fundamental role in the collection and preservation of electronic evidence.

Significant differences can be found between the EPdO/EPsO and mutual recognition instruments in place. The certificates for orders are to be notified directly to the service provider in the executing State, not to an authority there. The intervention of the executing authority is limited to one-off cases, such as notifications when the EPsO refers to data on persons not residing in its territory (Art. 7a (1) of the Council's general

approach), the withdrawal of immunities or privileges (Art. 7a (3) of the Council's general approach), and the transfer of orders and certificates to the executing authority in the event that the addressee fails to comply without giving reasons accepted by the issuing authority, in which case the executing authority will decide on recognition no later than five working days (Art. 14 of the Council's general approach).

European Production and Preservation Orders are certainly not an instrument in which an authority in the executing State recognises the order issued by the authority in the issuing State, without requiring any further formality, and executes it in the same way and under the same circumstances as if it had been ordered in the executing State – unlike the main principles for instruments of mutual recognition in criminal matters. Hence, the EPdO and the EPsO cannot as such be categorised as mutual recognition instruments,[15] but are instead instruments of judicial cooperation in criminal matters that require a "high level of mutual trust" for their proper functioning (Recital 11 of the Council's general approach). There is also no reference to the classic list of 32 offences for which the double criminality check –a common element in the mutual recognition instruments– will not be carried out. In other words, the EU's legislative approach is not an instrument of mutual recognition *per se*, but a new type of cooperation instrument based on advanced form of mutual trust.

In terms of the substantive contents of the proposal, the following aspects are worth highlighting: Orders should be necessary and proportionate, and they shall be issued in accordance with the principle of equivalence; they are restricted to criminal proceedings, but both orders can be issued for all criminal offences and for most types of data stored, such as subscriber data and access data, unless they relate to traffic data, transactions, and content. With regard to the latter data, and only specifically for the EPdO, the threshold is set such that the abstract penalty for the facts is at least three years' imprisonment[16] or that specific offences be related to or committed through cyberspace and terrorist offences. In the case of orders issued for the enforcement of a custodial sentence or a security measure involving deprivation of liberty, the duration of the deprivation of liberty must be at least four months (Arts. 5 and 6 of the Council's general approach).

III. The Issue of Proportionality

With regard to the application of the principle of proportionality, I believe that it should have a fundamental position and function, constituting the backbone of the whole system in the same way as the principle of necessity. According to the proposed Regulation, these principles will be applied in accordance with the CFR[17]. The fundamental rights of the subjects concerned shall be preserved, and the remedies guaranteed.[18] The issuing authority will be responsible for ensuring the compliance of these principles[19] (Recitals 12, 13, 24 and 46 of the Council's general approach). In the context of the e-evidence proposal, the application of the principles of proportionality and necessity requires an assessment in each individual case (Recital 24 of the Council's general approach). Given the invasive nature of the measure (Recitals 29 and 43 of the Council's general approach), this implies assessing whether the order is limited to what is strictly necessary in order to achieve its objectives, taking into account the impact on the fundamental rights of the person whose data are being requested. Personal data obtained through e-evidence may be processed only when necessary and proportionate for the purposes of prevention, investigation, detection, and prosecution of crimes; the application of criminal sanctions; and exercise of the right of defense (Recital 57 of the Council's general approach). Thus, the principle of necessity – despite having data protection implications – is used in the context of EPdO and EPsO primarily as part of the principle of proportionality (proportionality *stricto sensu*).

On many occasions, the proposal for a Regulation mentions the principle of proportionality and the impact on fundamental rights. Manifestations of the principle of proportionality are the guarantees provided for and specified in the provision on the EPdO in conjunction with traffic, transaction, and content data, since they are limited to offences involving at least a three-year maximum sentence (with the exception of cybercrime-

https://doi.org/10.30709/eucrim-2020-004

and terrorism-related offences).[20] While orders must include justification of necessity and proportionality according to the purpose of the particular proceedings, certificates will not include this information so as not to jeopardize investigations (Arts. 5, 6, and 8 of the Council's general approach). Respect for the principle of proportionality is also included in the system of confidentiality and providing information to the user (Art. 11 of the Council's general approach) and in the system of sanctions for service providers (Art. 13 of the Council's general approach).

If we apply the proportionality principle, there is a need for detailed regulation. It should take account of the penalty limits and other specific requirements to avoid the use of orders for minor offences, as in the case of other mutual recognition instruments, e.g. the EIO.[21] The effective application of the principle of proportionality could be at risk if orders are allowed for all types of criminal offences. In particular, the exception made to cybercrime-related offences involving the obtainment of traffic, transaction, and content data through EPdOs is too broad. Therefore, it follows that penalty limits and specific requirements fostering proportionality no longer constitute a concept with imprecise boundaries that allows for judicial discretion, as already pointed out in the legal literature.[22] The application of the principle of proportionality would help integrate the element of justice and promote the fairness of the entire system. This is necessary because there is an urgent need to reconcile the preservation of security within the AFSJ – which the new legislation on e-evidence is designed for – with the elements of freedom and justice in order to prevent these commitments from being deteriorated.[23] As the creation of an instrument for the transnational collection of electronic evidence is considered urgent, it is all the more necessary that both justice and freedom be put to good use in the AFSJ.

Reconciliation between security and justice is also a premise at the Council of Europe level. When interpreting the European Convention on Human Rights as regards access to data and the exchange of information between Member States for the purpose of combating transnational crime and terrorism, the ECtHR, on the one hand, recognises such access and exchanges as essential, due to the sophisticated methods of data evasion by criminal networks. On the other hand, the ECtHR defines the limits and proportionality of electronic surveillance. Given the difficulties States have in combating these forms of crime, the Court accepts the legitimate interest of Member States to take a firm position, but it also stresses that both access to and transfer of data must respect the principle of proportionality.[24]

It is also important to take these considerations seriously if it comes to the above-mentioned establishment of cooperation schemes on e-evidence at the international level. Indeed, they are reflected in the "Addendum to the Recommendation for a Council Decision" authorizing the opening of negotiations with a view towards concluding an agreement with the USA on cross-border access to e-evidence (see also I.).[25] This Addendum highlights the importance of respect for the principle of proportionality and due process. It stresses the relevance of the principles of necessity and proportionality when differentiating between the various categories of data, and it additionally advocates the application of these principles in the field of privacy and data protection.[26] The relevance of the principle of proportionality is also expressed in the "Addendum to the Recommendation for a Council Decision" to negotiate on a Second Additional Protocol to the Budapest Convention on Cybercrime;[27] it establishes that access to data shall be necessary and proportionate.[28]

IV. Conclusions

The transnational gathering of evidence remains a pending issue in the EU, which has largely shifted to electronic evidence. The link to the agreements that the EU is negotiating with the USA on electronic evidence is of particular interest. The agreement might bring civil law and common law closer together, which has been a burning issue in studies of the criminal procedure model for decades, e.g., as regards the question of whether common criteria can be established for rules on the exclusion of evidence. It was

argued in this article that the principle of proportionality must play an essential role, including the situation if third States are involved in the gathering of electronic evidence. It was also stressed that the EU proposal on e-evidence is not an instrument of mutual recognition *per se*, since the envisaged orders are not recognised and executed by judicial authorities in another EU Member State, but by representatives of (private) service providers. This new instrument therefore highlights the evolution of judicial cooperation in the EU. One should not lose sight of the necessary links that exist outside the EU, given the global dimension of the new and more serious forms of crime.

---

1. See "Proposal for a Decision of the Council on establishing the specific programme implementing Horizon Europe – the Framework Programme for Research and Innovation (2021–2027) – Partial General Approach", Council doc. 8550/19 of 15 April 2019. The "Civil Security for Society" cluster has a leading role in the new programme. The fundamental premise is a vision of Europe that protects, empowers, and ensures security.↩
2. COM(2018) 225 final and COM(2018) 226 final. For an analysis of the proposals, see also S. Tosza, "The European Commissions's Proposal on Cross-Border Access to E-Evidence", (2018) *eucrim*, 212–219.↩
3. Cf. point 6 of the Joint Declaration, available at: <https://www.consilium.europa.eu/en/press/press-releases/2016/03/24/statement-on-terrorist-attacks-in-brussels-on-22-march/>, accessed 20 May 2020.↩
4. The conclusions are available at: <https://www.consilium.europa.eu/media/24300/cyberspace-en.pdf>, accessed 20 May 2020.↩
5. Cf. <https://www.consilium.europa.eu/es/press/press-releases/2017/06/23/euco-conclusions/>, accessed 20 May 2020.↩
6. See <https://www.consilium.europa.eu/media/31666/st14435en17.pdf>, accessed 20 May 2020.↩
7. In this regard, <https://europa.eu/rapid/press-release_IP-18-3343_es.htm>, accessed 20 May 2020.↩
8. M. Jimeno Bulnes, "Capítulo XXXV. La prueba transfronteriza y su incorporación al proceso penal español", in: M. I. González Cano (ed.), *Orden Europea de investigación y prueba transfronteriza en la Unión Europea,* 2019, p. 719, pp. 759–761. The reference to the USA stands out as one of the fundamental clues to the legislative proposal, given that it receives the greatest number of requests from the EU, making it the impetus for and "leitmotiv" of the proposal.↩
9. For the CLOUD Act, see the article by J. Daskal, "Unpacking the CLOUD Act", (2018) *eucrim*, 220–225.↩
10. See <https://europa.eu/rapid/press-release_IP-19-2891_es.htm>, accessed 20 May 2020.↩
11. Cf. <https://www.consilium.europa.eu/en/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/>, accesed 20 May 2020↩
12. Cf. Council doc. 15292/18/19 of 12 December 2018; a version of the general approach of December 2018 supplemented by respective annexes was published on 11 June 2019, Council doc. 10206/19.↩
13. *Factsheet e-evidence,* <https://europa.eu/rapid/press-release_MEMO-18-3345_en.htm> , accessed 20 May 2020, and Arts. 1 and 2 of the general approach to Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters, Council doc. 10206/19 (11 June 2019) agreed by the Council (Justice and Home Affairs) at its meeting on 6 June2019. The references to the proposal for a Regulation allude to this latest version of June 2019.↩
14. Abs. 7 of the Proposal for a Directive (as agreed in the general approach of the Council, Council doc. 6946/19 of 28 February 2019, adopted on 8 March 2019).↩
15. As regards the European Investigation Order, there have even been questions as to whether this is really a mutual recognition instrument in the strict sense of the word; it seems that judicial cooperation in criminal matters needs to explore a reinterpretation of the mutual recognition principle and innovation as regards the forms of cooperation.↩
16. It is precisely the establishment of a minimum penalty limit with respect to access to data that is relevant for the application of the proportionality test. This is reflected in the ECJ judgment of 2 October 2018, case C-207/16, *Ministerio Fiscal*. In its Opinion on the seriousness of the offence and the principle of proportionality, the Advocate General noted that it is impossible to determine the proportionality solely on the basis of the abstract penalty, given the differences between the Member States. The new Regulation would therefore clarify this point.↩
17. As already noted by C. Cocq and F. Galli, "The Use of Surveillance Technologies for the Prevention, Investigation and Prosecution of Serious Crime", (2015), 41, *EUI Working Papers, Department of Law,* <https://cadmus.eui.eu/handle/1814/37885>, accessed 20 May 2020, 1, p. 48, with respect to the European regulatory framework on privacy, data retention affects the rights to privacy and the protection of personal data, fundamental rights under Arts. 7 and 8 CFR. Any limitation or intrusion must be clearly regulated, necessary, and proportionate to the purpose and must preserve the essence of the limited fundamental rights.↩
18. R.M. Geraci, "La circulazione transfrontaliera delle prove digitali in UE: La proposta di Regolamento e-evidence", (2019) *Cassazione penale,* 3, 1340, 1353. The execution of the orders affects a plurality of subjects, such as the person who owns the data, the service providers, and, possibly, third States.↩
19. M. Stefan and G. González Fuster, "Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters. State of the art and latest developments in the EU and the US", (2018) 7, *CEPS Papers in Liberty and Security in Europe,* <https://www.ceps.eu/ceps-publications/cross-border-access-electronic-data-through-judicial-cooperation-criminal-matters/> accessed 20 May 2020, 1, 30. It is particularly problematic that the offences to be affected by the proposed Regulation have not been precisely determined, as there is no verification of legality, necessity, and proportionality by the judicial authorities of the executing State.↩
20. Recitals 29,31,32 of the Council's general approach, *op. cit.* (n. 12).↩
21. See L. Bachmaier, "Prueba transnacional penal en Europa: la Directiva 2014/41 relativa a la orden europea de investigación", (2015) 36, *Revista General de Derecho europeo*, 15–19, noted this risk in the EIO, as minor offences are not excluded from its scope.↩
22. On this matter, T.I. Harbo, "Introducing procedural proportionality review in European Law", (2017) 30, *Leiden Journal of International Law*, 25, 25–26.↩

23. See E. Herlin-Karnell, "The domination of security and the promise of justice: on justification and proportionality in Europe's 'Area of Freedom, Security and Justice'", (2017) 8 (1) *Transnational Legal Theory*, 79, 83.↩
24. ECtHR, 13 September 2018, *Big Brother Watch and others v. the United Kingdom*, Application. nos. 58170/13, 62322/14 and 24960/15.↩
25. Cf. <https://data.consilium.europa.eu/doc/document/ST-9666-2019-INIT/en/pdf>, accessed 20 May 2020.↩
26. Cf. section III (Safeguards), paras. 1, 5.b) and 6.b).↩
27. Cf. <https://data.consilium.europa.eu/doc/document/ST-9664-2019-INIT/en/pdf>, accessed 20 May 2020.↩
28. See in particular I.b) (Objectives) and II.4 (Stronger safeguards for existing practices of transborder access to data).↩

Author statement

This article is part of the research project: "La evolución del espacio judicial europeo en materia civil y penal: su influencia en el proceso español", R+D Project, PGC2018-094209-B-I00, supported by the Spanish Ministry of Science, Innovation and Universities. It is also the result of a research stay the author completed as a visiting fellow at the European University Institute (Florence, Italy) in 2018, financed by the University of Seville's VI Research Plan.