European Union

The E-Evidence Package is Adopted: End of a Saga or Beginning of a New One?

*Stanisław Tosza**

I. Introduction

After a more than 5-years long saga, the so called 'e-evidence package' has finally been adopted. On 27 June 2023 the Council of the European Union approved a Regulation and a Directive on cross-border access to electronic evidence in the version of the texts, which the European Parliament had adopted on 13 June. Both acts were signed on 12 July and published in the Official Journal on 28 July.[1]

Thus ends the long legislative process, which saw different versions of the text, in particular the position of the Parliament significantly diverging from the original Commission's proposal,[2] a heated debate touching upon the very need of this legislation and fundamental questions of privacy,[3] the nature and future of transnational cooperation in criminal matters,[4] and the role of private actors in enforcement,[5] to name just some of the key questions. Several Council presidencies made efforts to find compromises during prolonged stalemates,[6] and at some points it looked as if the e-evidence package would be abandoned altogether. The need for a new legal framework was all too pertinent, however, and eventually the final text of the Regulation is not very divergent in essence from the original proposal presented by the Commission in April 2018.

It is impossible to present the entire e-evidence discussion and all the turns that the e-evidence legislative process took. The objective of this report is to present the main features of the new Regulation and the new Directive, its legal construction involving private actors as addressees of mutual recognition orders, its scope and procedural mechanism and briefly analyse its meaning for privacy and transnational cooperation in criminal matters. These aspects will be explained in turn, but first the report will examine why e-evidence is a challenge and why it requires a transnational legislative solution.

DOI: 10.21552/edpl/2023/2/11

* Stanisław Tosza, Associate Professor in Compliance and Law Enforcement, University of Luxembourg. For correspondence: <stanislaw.tosza@uni.lu>.

1 Documentation on the Regulation available at <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32023R1543> accessed 1 July 2023; Documentation on the Directive available at <https://eur-lex.europa.eu/eli/dir/2023/1544/oj> accessed 28 July 2023.

2 European Commission, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final 2018/0108 (COD) and Proposal of 17 April 2018 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 final, 2018/0107 (COD). The Parliaments Reports: Regulation: 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, 11.12.2020; Directive: Report 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, 11.12.2020.

3 Gloria González Fuster, Sergi Vázquez Maymir, 'Cross-border Access to E-Evidence: Framing the Evidence', CEPS 2020, available at: <https://www.ceps.eu/wp-content/uploads/2020/03/LSE2020-02_Cross-border-Access-to-E-Evidence.pdf> accessed 1 July 2023; Marine Corhay, 'Private Life, Personal Data Protection and the Role of Service Providers: The EU e-Evidence Proposal' (2021) 6 European Papers, 441-471.

4 Stanisław Tosza, 'All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order' (2020) 11 New Journal of European Criminal Law, 161-183; Katalin Ligeti, Gavin Robinson, 'Sword, Shield and Cloud: Toward a European System of Public–Private Orders for Electronic Evidence in Criminal Matters?' (2021) in: Mitsilegas, Vavoula (eds.), *Surveillance and Privacy in the Digital Age: European, Transatlantic and Global Perspectives*, Hart, 27–70.

5 Valsamis Mitsilegas, 'The Privatisation of Mutual Trust in Europe's Area of Criminal Justice: The Case of E-evidence' (2018) 25 Maastricht Journal of European and Comparative Law 3, 263–265, 264 f.; Stanisław Tosza, 'Internet service providers as law enforcers and adjudicators. A public role of private actors' (2021) 43 Computer Law & Security Review, 1-17.

6 See for instance the effort of the French Presidency of 16 June 2022: Note from the Presidency (Council doc. 10271/22, LIMITE, 16 June 2022), <https://data.consilium.europa.eu/doc/document/ST-10271-2022-INIT/en/pdf> accessed 1 July 2023.

II. The Need for Electronic Evidence – Context and Reasons for the E-Evidence Package

The essence of the problem of gathering electronic evidence lays in the combination of the unique opportunity for law enforcement offered by gathering of large amount of data by service providers and the outdated concept of territoriality significantly complicating the access to that data by law enforcement authorities across borders.

The nature of digital capitalism, which is based on amassing of large amounts of data, results in communication differing significantly from communication in the pre-Internet era (or better said pre-email and pre-instant messaging era). The snail post services did not gather copies of letters they transported (and in principle did not have access to them), neither did they gather metadata on those letters. Registered post was an exception and opening of the letters required a procedural measure, usually involving a judge.[7] To the contrary, Internet service providers (ISPs) today have access to the content of communication and accumulate huge amounts of metadata. Also, enormous amounts of traffic data of different kinds are gathered. All that data represents a treasure trove for law enforcement, who may use it as evidence of criminal offences. Given the increasing transfer of human activity to the digital world, this opportunity becomes a necessity.

At the same time, the existing legal framework hampered the possibilities to access the data. In its traditional approach – stemming from the Westphalian international law order – jurisdiction to enforce is limited to the territory of a state. In other words, the enforcement authorities cannot undertake any enforcement activities beyond the border of their own country. This rule was famously expressed in the seminal *Lotus* judgment of the Permanent Court of International Justice.[8] This limitation clashes with the nature of cyberspace and the Internet, which as such does not know the physical border with data flowing freely[9] around the globe between data centres. This means that all too often law enforcement would be confronted with relatively simple cases (e.g., national ones with victims and perpetrators being residents of their country, where also the offence took place), for which electronic evidence is necessary, but which is in the hands of a foreign service provider, potentially with a data centre in yet another country, if not circulating in pieces between various data centres.[10]

The rules of territoriality demand that in such cases law enforcement authorities request data by means of instruments of transnational (within the EU) or international (outside the EU) cooperation. Since 2017 the go-to instrument of cooperation within the European Union as regards exchange of evidence has been the European Investigation Order (EIO), which can be also used to issue transnational production orders.[11] It is applicable in all EU Member States, with the exception of Denmark (which does not participate in cooperation in criminal matters at all), and – importantly – Ireland (which may opt in to such instruments, but decided not to do so). For that latter Member State, which headquarters several important service providers for purposes of their European operations (e.g. Meta and Microsoft), the 1959 Mutual Legal Assistance Convention of the Council of Europe has to be used.[12] On the international level, it is also the mutual legal assistance (MLA) that forms the basis to request data from non-EU service providers. MLA is considered to be a cumbersome instrument requiring involvement of judicial authorities on both sides and communication through diplomatic channels.[13] For instance, it was estimated to take on average 10 months if data is sought from the US.[14]

7 See for instance §100 (1) StPO, Thomas Weigend, 'Germany' (2013) in: Katalin Ligeti (ed.), Toward a Prosecutor for the European Union. Vol. 1, Hart, 277.

8 S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10 (Sept. 7): "The first and foremost restriction imposed by international law upon a State is that – failing existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention".

9 At least apart from states which tightly control 'their' cyberspace.

10 Vivek Krishnamurthy, 'Cloudy with a Conflict of Laws: How Cloud Computing Has Disrupted the Mutual Legal Assistance Treaty System and Why It Matters', Berkman Klein Center Research Publication No. 2016-3 (18 February 2016), <https://ssrn.com/abstract=2733350> accessed 1 July 2023.

11 The deadline for the transposition of the European Investigation Order Directive was 22 May 2017.

12 See <https://www.gov.ie/en/policy-information/e5f87-mutual-legal-assistance/> accessed 1 July 2023.

13 European Commission, Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace, p. 5.

14 Richard A. Clarke et al., "Liberty and Security in a Changing World. Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies (2013), accessible at <https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf> accessed 1 July 2023, p. 227.

The clash between opportunity to gather electronic evidence and the impractical legal framework created frustration on the side of law enforcement,[15] which resulted in efforts to circumvent those difficulties, but as a result put in jeopardy in turn the protection of privacy and pushed the service providers into conflicting legal obligations.

On the one hand, law enforcement authorities developed a tendency to use voluntary cooperation. This form of non-binding requests may be used in particular to acquire non-content data from US providers, which may provide it (contrary to content data) to foreign law enforcement without a decision of a US judge. However, not only do the law enforcement authorities lack measures of compulsion in case of refusal, but also that form of cooperation does not offer a protective framework for persons concerned by those requests. As a result, the ISPs are *de facto* in charge of assessing the proportionality and legitimacy of requests, which is a typically public task.[16]

On the other hand, some countries, most notably Belgium,[17] decided to change the approach to territoriality. Belgium linked the duties of ISPs not with the location of headquarters or of the data, but with such matters as the language of the offered service (i.e., French and Dutch), the Internet domain (i.e., .be) and the effective targeting of local customers through advertisement. This approach, introduced through cases against Yahoo and Skype, was eventually adopted into the Code of Criminal Procedure.[18] However, while Belgium might issue compelling orders and threaten service provider with criminal sanctions for non-cooperation, they are still forbidden to produce content data without a decision of a US judge (i.e. outside of an MLA procedure) by virtue of US law,[19] which put them into a situation of conflicting legal obligations. Thus, it was not a surprise to see major providers, in particular Microsoft, advocating for a legislative change in order to eliminate that conflict.[20]

The first such change took place in the US, where the CLOUD Act was adopted in April 2018.[21] This act sets aside the blocking provisions thus allowing US service providers to produce content data to non-US authorities. However, for the blocking provision to disapply, there needs first to be an intergovernmental agreement between the US and the state, from which the requests for data would come.[22] So far, the US signed such an agreement with the UK and Australia, and negotiations are ongoing with Canada.[23] This system resulted in a question which has significant implications for the integrity of the EU's Area of Freedom, Security and Justice, namely whether the US would negotiate such an agreement with the EU as a whole or with individual Member States.

Around the same time, the European Commission issued the e-evidence package, with a dual aim. Firstly, its objective is to offer a new practical solution to gathering of electronic evidence within the European Union. It would offer a much faster instrument than the European Investigation Order, which would not require an intervention of the authorities of the Member State where the request is sent. Furthermore, Ireland would participate in this instrument, putting aside the MLA for electronic evidence as regards this country.[24] Secondly, it would 'Europeanise' the mat-

15 Which are itself exacerbated by the use of encryption and limited enforcement possibilities – Tosza, 'Internet service providers as law enforcers and adjudicators (n5).

16 See for instance the policies of Google <https://policies.google.com/terms/information-requests?sjid=14727799565052730419-EU> and Meta on handling government requests for data <https://about.meta.com/actions/safety/audiences/law/guidelines> accessed 1 July 2023.

17 Another example could be Germany, see Brodowski, "Die »Login-Falle« zur Identifizierung von Beschuldigten im Internet – eine »grundrechtsschonende und freiheitsorientierte« Ermittlungsmaßnahme?" Strafverteidiger (2022), 413-418.

18 Vanessa Franssen, 'The Belgian Internet Investigatory Powers Act - A Model to Pursue at European Level' (2017) 3 EDPL 534, 538-539.

19 18 U.S.C. §§ 2702.

20 John Frank, Mark Lange, Lani Cossette, "The eEvidence Proposal – A positive step forward", Microsoft EU Policy Blog, 18 April 2018, <https://blogs.microsoft.com/eupolicy/2018/04/18/the-eevidence-proposal-a-positive-step-forward/> accessed 1 July 2023.

21 Cf. on this in the context of the e-Evidence proposal eg. Mark D. Cole, Teresa Quintel, 'Transborder Access to e-Evidence by Law Enforcement Agencies' (May 11, 2018), University of Luxembourg Law Working Paper No. 2018-010, available at SSRN: <https://ssrn.com/abstract=3278780> accessed 1 July 2023.

22 Jennifer Daskal, 'Unpacking the CLOUD Act' (2018) 4 eucrim, 222-223.

23 Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime, available at: <https://www.justice.gov/criminal-oia/cloud-act-agreement-between-governments-us-united-kingdom-great-britain-and-northern#:~:text=The%20Agreement%20provides%20an%20efficient,consistent%20with%20its%20law%20and> accessed 1 July 2023; Australia: <https://www.homeaffairs.gov.au/nat-security/files/cloud-act-agreement-signed.pdf> accessed 1 July 2023; Canada, <https://www.justice.gov/opa/pr/united-states-and-canada-welcome-negotiations-cloud-act-agreement> accessed 1 July 2023.

24 Preamble to EPOR, Recital 100.

ter in a way as to give the EU the standing to negotiate with the US the agreement under the CLOUD Act.

Five years later, the package is adopted, so we are one step closer to achieving both objectives. As to the first one, its realisation depends on the effectiveness of the new instrument, which will be considered further below. As to the second objective, negotiations between the Commission and the US government, which formally started in 2019 and were frozen while waiting for the e-evidence package to be adopted, were unfrozen recently and presumably will be gaining speed in the nearest future.[25]

III. Unpacking the E-Evidence Package

1. A Regulation and a Directive – Two Instruments with the Same Goal

The 'Directive laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings' (further: the Directive) has an auxiliary role in this tandem. Its objective is to assure that for each service provider entering the scope of the Regulation there is at least one potential addressee of the newly created instruments of European Production or Preservation Orders. Thus, while it has only one precise objective, its fulfilment is a sine qua non condition of the efficacy of the new system. Those providers that are established in the EU shall designate at least one establishment, where such orders should be addressed. Those that are not established in the EU must appoint at least one legal representative who will be entitled to receive the order (Art. 3 of the Directive). Member States will have to ensure that the ISPs designate the establishment or appoint the representatives within three years from the entry into force of the Directive. They will also have to provide penalties for service providers that do not comply with the duties that the Directive provides for (Art. 5).

The 'Regulation on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings' (further: the Regulation or EPOR) is the main element of the package which creates the orders, provides the rule of their issuance, transmission to the service providers concerned, their execution and enforcement.

2. European Production and Preservation Orders – Scope, Procedure, Enforcement

The Regulation creates two orders: the European Production Order for production of electronic evidence, that is of the data that a service provider has, which may serve as evidence in criminal proceedings, and the European Preservation Order, which is a quick freeze instrument. European Production/Preservation Orders may be used only 'in the framework and for the purposes of criminal proceedings' as well as for execution of a 'custodial sentence or a detention order of at least four months' according to Art. 2 (2) EPOR. These proceedings may concern physical or legal persons, if, in case of the latter, the national legal order foresees corporate criminal liability (also laid down in Art. 2 (2) EPOR). Furthermore, orders cannot be used just for the purpose of providing mutual legal assistance to another Member State or a third country (Art. 2 (4) EPOR).

EPOR applies to service providers which offer services in the Union (Art. 2 (1)). The Regulation provides a detailed definition of the type of service providers falling into its scope in Art. 3 (3), which should be electronic communications services or other information society services enabling their users to communicate, internet domain name and IP numbering services or data storage or processing services. Those services do not need to be physically present in the EU (i.e., there is no need that they have headquarters or data centers in the EU). In order to fall into the scope of the e-evidence package they need to: 'hav[e] a substantial connection based on specific factual criteria' to a Member State where the service can be used. Such substantial connection may be based on the fact that 'there is a significant number of users in one or more Member States, or where there is targeting of activities towards one or more Member States' (Art. 3 (4) (b) EPOR).

EPOR applies only to four types of stored data, which also means that live communications are excluded. These can be grouped into two categories: on the one hand 'subscriber data' and 'data requested for the sole purpose of identifying the user', which are considered less intrusive, and on the other hand

25 See at <https://commission.europa.eu/news/eu-us-announcement-resumption-negotiations-eu-us-agreement-facilitate-access-electronic-evidence-2023-03-02_en> accessed 1 July 2023.

'traffic data' and 'content data'.[26] The categorisation of data is directly linked to the conditions of issuance of the European Production Orders and the circles of competent authorities. The first category can be requested by a judge, a court, an investigating judge or a public prosecutor as well as any other competent authority according to national law, but must be validated by one of the former authorities. As regards the traffic data (but not such that would fall into the category of data requested for the sole purpose of identifying the user)[27] and content data, the order cannot be issued by the public prosecutors solely. They would be able to issue the orders, but they would need to be validated by an (investigating) judge or a court (Art. 4 EPOR). As to the latter categories of data, the scope of the orders is also limited to 'criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least three years' and some additional offences listed in Art. 5 (4). That restriction will eliminate some offences from the scope of application of the orders for traffic and content data, but will arguably not limit its application only to serious offences as this threshold, especially in the more punitive criminal law systems, is relatively low.

The instrument of European Preservation Orders, as a less intrusive measure per se, is not subject to such restriction and may be issued for any offence and by all mentioned authorities including public prosecutors (Arts. 4 (3) and 5). It may be issued not only in view of a subsequent European Production Order, but also in view of requests for production of data via mutual legal assistance or a European Investigation Order (Art. 6 (2)).

The orders are transmitted to the service providers in form of standardised certificates according to Annexes to the Regulation (Art. 9, Annexes I and II). Upon reception of the certificate the service provider shall in all cases rapidly preserve the data. In case of the European Production Order, the data shall be transmitted to the requesting authority within 10 days from the reception of the certificate and within eight hours in emergency cases. Service providers may refuse to produce the data only for a limited number of reasons, mainly because the certificate 'is incomplete, contains manifest errors or does not contain sufficient information to execute [it]' (Art. 10 (6); 11 (5)) or because of the de facto impossibility due to circumstances not attributable to the addressee. Service providers shall also inform the issuing authority if they consider that the order 'could interfere with immunities or privileges, or with rules on the determination or limitation of criminal liability that relate to freedom of the press or freedom of expression in other media'[28].

If the service provider opts for refusing the order, it has to respond by means of Annex III to the Regulation. From this Annex it can be inferred that the service providers may also contest other aspects than those enumerated in Art. 11, namely whether the order was issued or validated by a competent authority, whether the request for traffic or content data was issued for offences to which orders for these types of data are limited, whether the service is covered by EPOR; they may also signal any other reason for non-compliance.

A particular procedure is foreseen if the order puts the provider in a situation of conflicting legal obligations due to applicable law of a third country (Art. 17 EPOR). The service provider shall signal that conflict in Annex III and the issuing authority is obliged to examine it. The initial version of this provision provided for a procedure of dialogue between the authorities of the issuing state and those of the third country with the outcome dependent on the response or silence of the authorities of the latter.[29] It did not seem feasible, however, to create an expectation of cooperation of third country authorities by means of an EU regulation, neither did it seem fair to make the fate of the provider dependent on the reaction of such an authority or lack thereof. The current solution, however, does not guarantee an elimination of the conflict as the authority may maintain the order regardless of the existing conflict. Nonetheless, Art. 17 provides a procedure for examination of that conflict and criteria according to which the decision shall be taken whether to maintain or lift the order.

There is one exception to the rule that the authorities of the enforcing state are not informed about the order: if the order concerns traffic or content data, a notification to the enforcing authority shall be sent simultaneously with the certificate addressed to the service provider. Prima facie, it seems to be a sig-

26 Their detailed definitions may be found in Art. 3 (9) - (12) EPOR.

27 For sake of brevity, references to traffic data here will be understood as not including data requested for the sole purpose of identifying the user.

28 Art. 11 (4) EPOR.

29 Art. 15-16 of the EPOR in the Commission's initial proposal.

nificant exception to the direct cooperation, but its effect will be significantly curtailed by the rule excluding from this obligation the category of national cases (i.e., where '(a) the offence has been committed, is being committed or is likely to be committed in the issuing State; and (b) the person whose data are requested resides in the issuing State') and it will be the issuing authority that shall assess whether it has reasonable grounds to believe that the case is national (Art. 8 (2) EPOR). It is important to note that this very authority also has the interest that the data is produced without further complications, which the notification may indeed create.

As the result of the notification, the enforcing authority may, within ten days, (partially or fully) block the transfer of data or limit its use (Art. 12 EPOR) based on enumerated criteria: existence of immunities or privileges, the principle of ne bis in idem, lack of double criminality (with the exception of offences listed in Annex IV to the Regulation) and – probably the most important one – a manifest breach of a relevant fundamental right as set out in Article 6 TEU and the Charter. The latter ground for refusal can only be evoked 'in exceptional situations', a seemingly illogical expression, which would suggest that if the breach is systematic that ground for refusal cannot be used (Art. 12 (1)).

The notification in this version – which did not exist in the Commission's proposal – is a compromise product resulting from intense debate as it was one of the most contentious points of the negotiations of the e-evidence package. In particular the Parliament advocated its much more extensive use.[30] Some authors also proposed transmitting the notification to other involved Member States, such as the country which the person whose data is being sought has the nationality of.[31] As this idea was excluded, it remains to be seen whether the enforcing authorities will engage in systematic review of notifications not involving any interests linked to their own country (i.e., where their nationals are not concerned).

An element that was added relatively late in the negotiations is the so called 'decentralised IT system', through which all communication and data exchange between the authorities and the service providers shall take place for the sake of security.[32] Member States will provide their national IT system for that purpose, but they also may choose to apply the system that the Commission shall create, maintain and develop.[33]

Two elements of the Regulation shall assure compliance with the orders in case of refusal to produce data by a requested service provider. Firstly, non-cooperation of the service provider triggers the enforcement procedure, which transforms the order into a 'classic' mutual recognition instrument: the issuing authority may request the authority of the Member State of the provider to enforce the order. In that case the enforcing authority will have at its disposal grounds for refusal, which concern the validity of the issuing of the order, immunities and privileges, impossibility on the side of the provider and fundamental rights considerations formulated in the same way as for the procedure of notification (Art. 16 EPOR).

Secondly, a non-compliant service provider shall be subject to pecuniary penalties. The Member States have to set the level for these in national law. The Regulation's input on this matter is limited to imposing the obligation that among the available sanctions there is a pecuniary penalty of 'up to 2 % of the total worldwide annual turnover of the service provider's preceding financial year' (Art. 15 (1)).

3. The Regulation as a Legal Revolution and a Quantum Leap of Mutual Trust

The main premise of the EPOR is that competent authorities will be entitled to issue binding requests to service providers offering services within the EU[34] regardless of their place of establishment or the physical location of the data (or in case of lack of precise location).

What is ground-breaking is that the Regulation sets aside the traditional strong approach to sovereignty, because law enforcement authorities of one Member State will be allowed to issue orders that are transmitted directly to private actors in a different Member State and which will have to be executed

30 See in particular Art. 9 of the report of the Parliament.

31 Theodore Christakis '"Big Divergence of Opinions" on E-Evidence in the EU Council: A Proposal in order to Disentangle the Notification Knot' (2018) Cross-Border Data Forum, <https://www.crossborderdataforum.org/big-divergence-of-opinions-on-e-evidence-in-the-eu-council-a-proposal-in-order-to-disentangle-the-notification-knot/> accessed 1 July 2023.

32 Art. 19-26 EPOR.

33 Art. 22 EPOR.

34 As Denmark does not participate in the Regulation, service providers will have to choose any other Member State: Art. 3 (1) (b) and (c) of the Directive.

without any involvement of the authorities of that latter Member State (with limited exceptions that will be explained below). This is actually in accordance with the Lotus principle as explained above, as the limitation to the sovereignty approach is done by a 'treaty'. Yet, we have not seen such a self-limitation of sovereignty in matters related to criminal justice in any other instruments of cooperation within the EU or the Council of Europe so far.

Two elements of this design are revolutionary. Firstly, the instrument is no longer based on the traditional concept of territoriality, but draws consequences from the difficulties this approach generates, its outdatedness and the loss of location. It also takes inspiration from the national solution such as the Belgian one. The duty is now linked with the criterion of 'offering services in the Union' (Art. 1 (1) EPOR).

Secondly, it is based on mutual recognition, but redefines the nature of transnational cooperation based on this principle. The Regulation's legal basis is Art. 82(1) TFUE, which has served as a basis for adoption of numerous directives or framework decisions providing mutual recognition of different procedural measures (e.g., arrest warrants, investigation orders or freezing orders and confiscation orders). It will only be the second *regulation* in the series of mutual recognition instruments, so it will be directly applicable in the Member States, although a few critical matters were left to be specified at the national level.

What is more important is that all these previous instruments were based on direct cooperation between law enforcement authorities. With EPOR, for the first time, law enforcement in one Member State will be able to issue a compelling order addressed to a private actor in another Member State. Most of the interaction will not involve the authorities in the Member States where the provider has the designated establishment or where its representative is located. This raises the question whether Art. 82 (1) TFUE is the correct legal basis for the adoption of such an instrument, which one may expect to result in a challenge of the validity of the EPOR in front of the Court of Justice of the European Union (CJEU). A detailed analysis of this problem is beyond the scope of this report,[35] but three arguments may be raised to demonstrate that the legal basis can be saved.

Firstly, Art. 82 (1) TFUE does not define the concept of mutual recognition, neither does it say that it has to take place within an interaction between two authorities (although the term 'judicial cooperation' arguably implies it). One can accept that the recognition takes place tacitly, as the Member States accept that an order from another Member State enters their sovereign sphere and is executed by an obliged private actor. Secondly, in case of non-compliance, the order will turn into a traditional mutual recognition instrument with the authorities in the Member State of the provider bearing the responsibility for the enforcement of the order (that is why they are called 'enforcing State' and 'enforcing authority').[36] Thirdly, mutual recognition is a rather flexible concept, developed initially in the framework of the internal market, it has been translated into the cooperation in criminal matter only 25 years ago,[37] and as such does not seem to be prevented from further adjustment to the needs of enforcement in light of technological developments.

What is more fundamental is that this construction – eliminating the control of the authorities of the Member State where the request is sent – presupposes a higher level of mutual trust between the States. The general assumption of mutual recognition has been that the Member States can trust each other assuming that all of them offer the same – high – level of fundamental rights guarantees, mostly as a result of long term membership in the Council of Europe with established jurisprudence of the European Court of Human Rights, and as a result should be predisposed to execute orders coming from other Member States with only limited scope for their verification.[38] This trust has been put under question in the past years in the context of the (EU's) European Arrest Warrant, firstly in the Aranyosi/Căldăraru judgment of the CJEU on prison conditions,[39] and later as regards the independence of the judiciary in

35 See for instance, Martin Böse, 'An assessment of the Commission's proposals on electronic evidence, Study requested by the LIBE committee of the EU Parliament' (2018) 36; Elodie Sellier, Anne Weyembergh, 'Criminal procedural laws across the European Union – A comparative analysis of selected main differences and the impact they have over the development of EU legislation, Study requested by the LIBE committee of the EU Parliament' (2018) 31.

36 Art. 3 (16) and (17) EPOR.

37 Presidency Conclusions, Tampere European Council, 15 and 16 October 1999, point 33. Art. 82 (1) TFEU.

38 André Klip, 'European Criminal Law. An Integrative Approach' (2021) Intersentia 4th ed., 473-474.

39 Joined Cases C-404/15 and C-659/15 PPU, Aranyosi/Căldăraru, EU:C:2016:198.

Poland.[40] Curiously, in parallel to the shrinking mutual trust between the Member States an instrument is adopted that requires in effect a quantum leap of that trust.

This tension was very present in the course of negotiations, with the Parliament proposing a special procedure regarding Member States that are subject to the rule of law-procedure of Article 7 of the TEU, which would have required an explicit written approval of the executing authority for the ISPs before the transfer of data.[41] This would mean in practice that for instance Irish authorities would need to approve all requests issued by the Polish or Hungarian authorities as long as Poland and Hungary are subject to this procedure. This proposal was eventually abandoned, and it remains to be seen how the Member States react to the question of orders issues by the authorities in countries where the rule of law is deficient. European Arrests Warrants in the past were not executed for such reasons,[42] and more recently European Investigation Orders were also examined from the same perspective.[43] However, in those cases the authorities would receive the order first and examine whether there is a rule of law deficiency (of the order or the issuing authority) justifying a refusal.[44] As far as the European Production/Preservation Orders are concerned, they will be received in principle, by a private actor – a service provider – that will have to assess whether to execute it without any further ado or refuse its execution thus triggering the authority in their Member State. Only in exceptional cases will the enforcing authority be informed at the moment of issuing the order, but most of the orders will land on the desks of the ISPs only.

Service providers do not really have a legal basis for such a refusal, so they will have to deliberately choose non-compliance (and risk being subject to financial penalties), if they consider that there are good reasons for questioning the order. This also turns service providers in effect into guardians of individuals' fundamental rights, a task usually reserved for public authorities, but increasingly transferred to private actors.[45]

IV. Protection of Privacy and Data Protection

In its Art. 1 (3) EPOR declares: 'This Regulation applies without prejudice to fundamental principles, in particular the freedom of expression and information, including the freedom and pluralism of the media, respect for private and family life, the protection of personal data, as well as the right to effective judicial protection.' Whether the Regulation will realise this declaration remains to be seen.

One of the main concerns of that act was whether it would be compliant with the criteria set up by the CJEU in the Digital Rights Ireland and Tele2 Sverige judgments.[46] An analysis from that perspective would go beyond the scope of this report.[47] One has to notice, however, that at no point does the Regulation formulate any general retention obligation, and the data is requested to be used in a concrete criminal case and not for any general or preventive purposes.[48] More questionable is the limitation of the requests for traffic and content data, which can be issued only to offences that are indeed more serious,

40 Case C-216/18 PPU, LM, EU:C:2018:586. For the follow-up jurisprudence see: Michiel Luchtman, Stanisław Tosza, 'How to deal with rule of law-concerns in surrender procedures?' (2023) in: Michiel Luchtman et al (eds.), Of swords and shields: due process and crime control in times of globalization - Liber amicorum prof. dr. J.A.E. Vervaele, Eleven, 453-461.

41 Art. 9 (2a) EPOR according to the Parliament's position, <https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_EN.html> accessed 1 July 2023.

42 Michiel Luchtman and Stanislaw Tosza (n 40).

43 Opinion of AG Bobek delivered on 29 April 2021 in Case C-852/19, Gavanozov II, ECLI:EU:C:2021:346, para 71ff.

44 Art. 1 (3) of the European Arrest Warrant Framework Decision and Art. 1 (4) of the European Investigation Order Directive include a general rule of law clause, which was used as a basis for the refusals to execute the respective orders, as general rule of law considerations are not part of the lists of grounds for refusal. The ECJ established a two-pronged test in the Aranyosi/Căldăraru judgment, according to which there must be general and systematic fundamental rights' deficiencies and that there are substantial grounds to believe that the individual in question will be affected by these deficiencies if the order is executed. The follow-up jurisprudence continue to apply it in other mutual recognition cases concerning rule of law deficiencies.

45 Tosza, Internet service providers as law enforcers and adjudicators (n5).

46 Joined Cases C-203/15 Tele2 Sverige AB v Post-och telestyrelsen andC-698/15 Secretary of State for the Home Department v Tom Watson and Others [2016] ECLI:EU:C:2016:970, para 108; cf. on this Gavin Robinson, 'The European Commission's e-Evidence Proposal' (2018) 3 EDPL 351.

47 See in that respect Gavin Robinson, 'Effective Data Protection and Direct Cooperation on Digital Evidence in Criminal Matters' in: Vanessa Franssen, Stanislaw Tosza, The Cambridge Handbook of Electronic Evidence, CUP, forthcoming.

48 As underlined by the Commission: Draft EPO Regulation, Explanatory Report, 15.

but are not only the category of serious offences, as national laws will easily provide examples of offences of medium gravity at best, which will fall into the scope of the instrument.[49] The very lack of a data retention regime may notably also weaken the effectiveness of this instrument, but it was excluded, apart from the quick freeze offered by the European Preservation Order, from its scope. The Regulation also does not provide any obligation to decrypt data as clearly stated in the preamble.[50]

EPOR provides for an article on effective remedies that shall be provided at the national level and shall include the possibility to question the necessity and proportionality of the order.[51] This remains one of the biggest open questions of the new system as the Regulation sets only some conditions on those remedies, but otherwise it is for the Member States to fill the details. The Regulation mandates that 'a suspect or an accused person [...] shall have the right to effective remedies during the criminal proceedings in which the data were being used.'[52] The right to remedies provided by virtue of the Regulation shall be also without prejudice to the rights stemming from the GDPR or the Law Enforcement Directive (LED).[53]

The effectiveness of the remedies will be linked with the information that the person whose data are being requested receives on the fact that the order was issued. The issuing authority shall inform that person about the production of data on the basis of a European Production Order without undue delay (Art. 13 (1) EPOR). However, the issuing authority may delay, restrict or even omit to inform that person for reasons which concern inter alia the interest of the investigation, more generally combatting crime or national interests. The Regulation borrows these criteria from Article 13(3) LED, and as can be seen they are sufficiently broad to offer wide possibilities of not informing persons concerned about the transfer of their data through the orders, thus limiting their ability to complain against them.[54]

V. Conclusion and Outlook

As the e-evidence legislative saga seems to be coming to an end, the question to be asked at this point of time is whether we are at the finishing line, or rather at the beginning of a new saga (or maybe just at a turning point of an ongoing one). The new Regulation will enter into force 20 days after the publication in the Official Journal, but will start to apply only three years afterwards. These three years are meant to give sufficient time to adopt the national legal frameworks to the new paradigm of mutual recognition where necessary, adopt national rules on aspects which the Regulation delegates to the Member States and create the decentralised IT system for exchange of data, an aspect which may prove to be highly complex in practice. Finally, the Directive has to be implemented, for which the Member States have 30 months.

The efficiency of this instrument will depend on several factors, which are still left open. Some of them are inherent to the e-evidence package. These are, in particular, the system of sanctions (and their practical application) for non-compliant service providers as well as the effective remedies. Factors external to this legislation will also have crucial impact on the new system. The prime issue in that respect is the success of the negotiations with the US under the CLOUD agreement. Already in June 2019, the Council authorised the European Commission to enter into the negotiations with the US, but their progress was impeded by the prolonged debate on the e-evidence package. As soon as the political agreement on the latter was reached, the negotiations were unfrozen.

The Regulation does not touch upon a number of issues, which were already mentioned above: data retention, encryption, admissibility of evidence. They will be, however, of key importance for the possibil-

49 E.g. the Polish Criminal Code punishes with imprisonment of up to 3 years someone who prevents or hinders official activities of a person authorised to carry out inspections in the field of environmental protection or a person adopted to help that person. Similar provisions applies to a person hindering official labour law inspections (Art. 225 § 1 and § 2 respectively).

50 Recital 20.

51 Art. 18 (2) EPOR.

52 Art. 18 (1) EPOR.

53 Art. 18 (1) EPOR, Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L 119/89.

54 On Art. 13 LED, see Gloria González Fuster, 'Article 13 Information to be Made Available or Given to the Data Subject' (2023) in: Eleni Kosta and Franziska Boehm, The EU Law Enforcement Directive (LED). A Commentary. OUP.

ity to acquire and use the data as evidence. A recent academic initiative resulted in a proposal for harmonization of rules on admissibility of evidence, but whether the EU Commission will propose legislation in this area remains unclear.[55]

Furthermore, in parallel to the implementation of the e-evidence package the ratification process of the Second Protocol to the Budapest Convention on Cybercrime will continue. It its Art. 6 and 7 this Protocol to the Cybercrime Convention also provides direct cooperation with service providers, although limited only to domain name registration information and subscriber information.[56] It may, however, have a much more global impact, if most of the State Parties to the Convention (which go well beyond the Member States of the Council of Europe) decide to join this Protocol as well.

One may expect litigation on key aspects of the e-evidence package. Already the use of the legal basis was questioned in the debates leading up to its adoption, so it would not be a surprise if the CJEU is called upon to assess its validity. Another issue, which may generate litigation is the question of the continuous use of more convenient national law instruments, where they exist, instead of the European Production Orders.

Finally, more general questions, which will be looming over the process of implementing the e-evidence package concern its impact on the use of evidence in criminal investigations for which one can ask whether e-evidence will become the preferred form of evidence, if it is easier to acquire, as well as the overall paradigm of transnational cooperation in criminal matters as this model of direct cooperation could be extended to other procedural measures, for instance concerning live communications.[57]

---

55 See ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings (2023) <https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Proposal_for_a_Directive_on_Mutual_Admissibility_of_Evidence_and_Electronic_Evidence_in_Criminal_Proceedings_in_the_EU.pdf> accessed 1 July 2023.

56 Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224).

57 Stanisław Tosza, 'All evidence is equal…' (n4), 181–182.