Articles

Studia Iuridica Lublinensia vol. 33, 5, 2024
DOI: 10.17951/sil.2024.33.5.237-260

Stanisław Tosza
University of Luxembourg, Luxembourg
ORCID: 0000-0002-3265-1460
stanislaw.tosza@uni.lu

Electronic Evidence after E-evidence Package's Adoption: Challenges for Application and Unresolved Problems

Pakiet o dowodach elektronicznych. Nierozwiązane problemy oraz wyzwania związane z jego zastosowaniem

ABSTRACT

On 12 July 2023, the European Union adopted the e-evidence package after five lengthy years of negotiating this controversial legislation. This package introduces a new model of cooperation to ensure transnational access to data for criminal investigations and prosecutions. The new model aims to offer a more efficient way of requesting data from service providers, often located in different countries, by allowing direct requests to Internet service providers active within the European Union. This approach will bypass the authorities in the Member States where the request is received. Providers will be required to designate at least one establishment or representative capable of receiving and responding to such requests promptly, and authorities will be permitted to send their requests directly to these designated entities. While the adoption of the e-evidence package marks a crucial step forward, its effectiveness, viability and practical application depend on several unresolved issues left to the Member States, or not addressed at all, and on reaching an agreement with the U.S. under the so-called CLOUD Act. This article aims to present the current state of play, examine these remaining issues and assess their impact on the final design of the system for accessing electronic evidence in the European Union.

Keywords: electronic evidence; European Production Order; Internet service providers; encryption; admissibility of evidence; European Investigation Order

---

CORRESPONDENCE ADDRESS: Stanislaw Tosza, PhD, Associate Professor in Compliance and Law Enforcement, Director of the Bachelor in Law, Secretary General of the International Association of Penal Law (AIDP/IAPL), Faculty of Law, Economics and Finance, University of Luxembourg, 4 rue Alphonse Weicker, L-2721 Luxembourg.

INTRODUCTION

On 12 July 2023, the European Union adopted the so-called e-evidence package ending five years of negotiations and an even longer reflection period on how to adjust the rules of transnational cooperation to the era of dominant digital communication in order to allow law enforcement to access data in possession of service providers for the purposes of criminal investigations.[1] The need for this reflection and eventually legislative intervention stems from the clash of the traditional principle of territoriality with the borderless nature of cyberspace.[2]

While the principle of territoriality limits the actions of law enforcement to the remits of state borders, data roams freely in countries that do not limit that freedom. In particular, EU Member States have refrained from imposing localisation obligations,[3] which means that data of European users may be stored outside the European Union.[4] Moreover, most of the major providers are U.S. companies (e.g. Google or Meta) and thus access to data held by those companies is subject to U.S. law. At the same time, the need for data in order to effectively investigate and combat crime has been only increasingly.

The frustration of law enforcement resulting from these problems culminated in several high-profile cases in the U.S.[5] and in Europe (precisely in Belgium),[6] which precipitated the need for new legislation. Three new major acts resulted from this need adopted within three different fora: the above-mentioned e-evidence package, the CLOUD Act in the U.S. and the Second Protocol to the Cybercrime Convention.

While the adoption of these instruments – especially as regards the lengthy negotiations of the e-evidence package – may have been felt as a culmination point of addressing the problem of gathering data for criminal investigations from service

---

[1] I am very grateful to Martina Siclari for her valuable help in conducting research for this article. All mistakes remain my own.

[2] U. Sieber, C. Neubert, *Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty*, "Max Planck Yearbook of United Nations Law Online" 2017, vol. 20, p. 239; J. Daskal, *The Un-territoriality of Data*, "The Yale Law Journal" 2015, vol. 125, pp. 326–398; S. Tosza, *Internet Service Providers as Law Enforcers and Adjudicators: A Public Role of Private Actors*, "Computer Law & Security Review" 2021, vol. 43.

[3] Contrary to such countries as Turkey or Russia. See S. Bilgiç, *Digital Evidence Collection in Turkey*, [in:] *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, eds. V. Franssen, S. Tosza, 2025 [forthcoming]; M. Filatova, O. Kostyleva, T. Alekseeva, *Cooperation of Service Providers in Criminal Investigations in the Russian Federation*, [in:] *The Cambridge Handbook…*

[4] This possibility may be limited by data protection law, however.

[5] Decision of the U.S. Court of Appeals – Second Circuit of 14 July 2016, *Microsoft Corp. v. United States* (so-called Microsoft Ireland Case), 829 F.3d 197.

[6] V. Franssen, *The Belgian Internet Investigatory Powers Act – A Model to Pursue at European Level?*, "European Data Protection Law Review" 2017, vol. 3(4), p. 534.

providers, even if numerous fundamental rights' questions remained controversial.[7] However, the system offered by the e-evidence package does not function yet and depends on national legislation in every EU Member State, which is part of this system,[8] an agreement with the U.S. and technical capacity that still needs to be provided. The effectiveness, legitimacy and practical success of the e-evidence package depend on these acts.

The objective of this article is to present these remaining issues. It starts by presenting the state of play and the next steps as regards legislation on cross-border gathering of electronic evidence. The article with then focus on the challenges that national legislators will have to face in adopting national law to the e-evidence package and on issues which are unresolved by the e-evidence package, but will affect the gathering of electronic evidence in the EU, before offering concluding remarks.

STATE OF PLAY AND NEXT STEPS

The rules on the process of gathering electronic evidence are currently in a transitional phase. Although new solutions have been adopted, considerable action is still needed from legislators and state parties for them to become operational. Meanwhile, the old solutions remain in use, a situation that is expected to last until summer 2026. In order to paint the full picture of the problem, it is necessary to first explain the reasons why electronic evidence creates such a significant inter- and transnational cooperation challenge, examine what the solutions still in place are and what the solutions are that should soon come into practical effect.[9]

---

[7] S. Tosza, *Mutual Recognition by Private Actors in Criminal Justice? E-evidence Regulation and Service Providers as the New Guardians of Fundamental Rights*, "Common Market Law Review" 2024, vol. 61(1), pp. 139–166; V. Mitsilegas, *The Privatisation of Mutual Trust in Europe's Area of Criminal Justice: The Case of E-evidence*, "Maastricht Journal of European and Comparative Law" 2018, vol. 25(3), pp. 263–265; M. Böse, *An Assessment of the Commission's Proposals on Electronic Evidence*, 2018, https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf (access: 16.12.2024).

[8] Denmark does not participate in cooperation in criminal matters. Ireland opted in to the e-evidence Regulation.

[9] This section presents a succinct summary of the current state of play. For more detailed examination, see S. Tosza, *The E-evidence Package Is Adopted: End of a Saga or Beginning of a New One?*, "European Data Protection Law Review" 2023, vol. 9, pp. 163–172; idem, *Mutual Recognition…* This section uses research from these two publications, summarizing and updating its findings to the current situation. See as well contributions to the book: V. Franssen, S. Tosza (eds.), *op. cit*. For an introduction to the topic in Polish, see in particular M. Kusak, *Dostęp do danych elektronicznych dotyczących treści w postępowaniu karnym – wyzwania krajowe i międzynarodowe*, "Gdańskie Studia Prawnicze" 2024, no. 2, pp. 72–88; S. Tosza, *W poszukiwaniu dowodów elektronicznych – europejski nakaz wydania dowodów elektronicznych oraz inne narzędzia międzynarodowego pozyskiwania danych dla potrzeb postępowania karnego*, "Gdańskie Studia Prawnicze" 2024, no. 2, pp. 37–55.

The challenge of gathering electronic evidence lies in the tension between the vast amounts of data collected by service providers and the outdated concept of territoriality, which complicates cross-border access to this data by law enforcement. Unlike traditional communication methods, where physical mail did not retain metadata or content, modern Internet service providers store extensive communication data and metadata, creating valuable evidence for criminal investigations. However, the current legal framework, rooted in the principle that enforcement jurisdiction is confined to a state's territory,[10] restricts law enforcement's ability to access data stored abroad. This territorial limitation clashes with the borderless nature of the Internet, where data flows globally, often leaving law enforcement in need of foreign-held evidence for domestic cases.[11]

Within the EU, the European Investigation Order (EIO) has been the primary tool for cross-border evidence requests since 2017, though it's not applicable in Denmark or Ireland, the latter being home to major service providers. Internationally, mutual legal assistance (MLA) remains the standard method for data requests, but it is a slow and cumbersome process, requiring the use of diplomatic channels next to judiciary proceedings,[12] on average taking around a year to receive data from non-EU service providers, particularly from the U.S.[13]

The conflict between the opportunity to gather electronic evidence and an outdated legal framework has led to frustration of the law enforcement authorities, resulting in efforts to bypass legal challenges, but also raising concerns about privacy and putting service providers in difficult legal positions. Law enforcement increasingly relied on voluntary cooperation with U.S. providers to obtain non-content data.[14] However, this method lacks enforcement power and fails to protect individuals' rights, leaving service providers to determine the legitimacy of requests on their own.

---

[10] Judgment of the Permanent Court of International Justice on 7 September 1927, *SS Lotus (Fr. v. Turk.)*, Publications of the Permanent Court of International Justice, Series A.-No. 70: "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".

[11] J. Daskal, *The Un-territoriality of Data…*

[12] European Commission, *Non-Paper: Progress Report Following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace*, Brussels, 7.12.2016, https://data.consilium.europa.eu/doc/document/ST-15072-2016-REV-1/en/pdf (access: 16.12.2024), p. 5.

[13] R.A. Clarke, M.J. Morell, G.R. Stone, C.R. Sunstein, P. Swire, *Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies*, 12.12.2013, https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (access: 16.12.2024), p. 227.

[14] 18 U.S.C. § 2702 forbids U.S. providers to provide data to foreign law enforcement without an intervention of a U.S. judge. This so-called "blocking provision" does not apply, however, to non-content data.

The frustration of law enforcement was palpable on both sides of the Atlantic. In the U.S., it culminated with the Microsoft Ireland case, where U.S. authorities' efforts to obtain email content from Microsoft were hampered by the fact that the emails in question were stored in the U.S.[15] On the European side, the most active in that respect were the Belgian authorities, where a string of jurisprudence led to the redefinition of territoriality by linking ISPs' obligations – regardless if foreign – to local factors like the use of language (French or Dutch) and advertising targeting local customers.[16] This approach, however, created legal conflicts, particularly for U.S. providers, which, as indicated, restricts the production of content data without judicial approval.

At that point, it was clear that new solutions needed to be adopted, as also major service providers, such as Microsoft, started to advocate for legislative changes. This led to the adoption of three key legislative initiatives: the U.S. CLOUD Act, the EU e-evidence package, and the Second Protocol to the Cybercrime Convention.

The U.S. CLOUD Act was the first to be enacted already in March 2018.[17] It allows U.S. providers to share content data with non-U.S. authorities, provided that there is an intergovernmental agreement in place. This latter condition results in the fact that despite being in place for more than six years already it has not produced yet a significant change to the rules of international gathering of electronic evidence. While the U.S. signed a few of such agreements, e.g. with the UK and Australia,[18] the agreement with the EU is still in the pipeline.

The question that was open at the time of the adoption of the CLOUD Act was whether the U.S. would negotiate such agreements with each EU Member State individually or with the EU as a whole. The latter solution was clearly preferable from the perspective of celerity and uniformity of rules within the Area of Freedom, Security and Justice. The fact that the EU proposed the e-evidence package (in 2018) positioned it as the partner for such negotiations.[19] Negotiations with the U.S. were

---

[15] U.S. Court of Appeals for the Second Circuit, in re *Microsoft Corp*. (so-called *Microsoft Ireland Case*), 829 F.3d 197 (2nd Cir. 2016).

[16] See the Belgian cases of Yahoo and Skype analysed by V. Franssen, *The Belgian Internet…*

[17] Clarifying Lawful Overseas Use of Data Act – CLOUD Act, S. 2383, 115th Cong. § 2(1)–(2) (2018) (codified at 18 U.S.C. §§ 2713, 2523 (2018).

[18] U.S. Department of Justice, Cloud Act Agreement between the Governments of the U.S., United Kingdom of Great Britain and Northern Ireland, https://www.justice.gov/criminal/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 (access: 16.12.2024); Agreement between the Government of Australia and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, https://www.homeaffairs.gov.au/nat-security/files/cloud-act-agreement-signed.pdf (access: 16.12.2024).

[19] J. Daskal, *Unpacking the CLOUD Act*, "Eucrim" 2018, no. 4, pp. 220–225; K. Woods, P. Swire, *The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems*, 6.2.2018, https://www.lawfaremedia.org/article/cloud-act-welcome-legislative-fix-cross-border-data-problems (access: 16.12.2024).

authorized in 2019, but had to be frozen due to lengthy talks on the e-evidence package. Once the e-evidence package was adopted in 2023, the negotiations swiftly restarted.[20] At the moment of writing these negotiations are ongoing and not much is known about their details. As will be shown below, the existence of the agreement between the EU and the U.S. is crucial for the success of the e-evidence package, as without it the package's efficacy will be significantly hampered.

Almost at the same time when the U.S. Congress enacted the CLOUD Act, the European Commission introduced the e-evidence package with two objectives.[21] In the first place, it was supposed to offer a more practical solution in order to acquire data for evidence in criminal proceedings within the EU and include into its scope all service providers active in the EU, regardless if they are European or not. The second objective of the package, as already mentioned, was to place the EU as the negotiating partner with the U.S. in the context of the CLOUD Act.

It took very lengthy five years to adopt the e-evidence package, and the legislative procedure ended on 12 July 2023. The package is composed of two instruments: a Directive and a Regulation, out of which the latter is the crucial one.

The Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings[22] serves a supporting role in the new e-evidence framework. Its main objective is to ensure that every service provider subject to the Regulation has a designated recipient for European Production or Preservation Orders. EU-based providers must designate an establishment to receive such orders, while non-EU providers must appoint a legal representative. The Directive also includes penalties for non-compliance with its duties.

The Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings[23] is the main element of the e-evidence package. It is by virtue of this Regulation that the European Production Order is

[20] See European Commission, *EU-U.S. Announcement on the Resumption of Negotiations on an EU-U.S. Agreement to Facilitate Access to Electronic Evidence in Criminal Investigations*, 2.3.2023, https://commission.europa.eu/news/eu-us-announcement-resumption-negotiations-eu-us-agreement-facilitate-access-electronic-evidence-2023-03-02_en (access: 16.12.2024).

[21] Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, Strasbourg, 17.4.2018, COM/2018/225 final; 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, Strasbourg,17.4.2018, COM/2018/226 final.

[22] OJ EU L 191/181, 28.7.2023, hereinafter: the Directive.

[23] OJ EU L 191/118, 28.7.2023), hereinafter: the Regulation or EPOR.

created and it provides different rules regarding its issuance, interaction with the service provider, execution and enforcement.

The Regulation introduces two key instruments for criminal investigations: the European Production Order and the European Preservation Order. The European Production Order allows law enforcement to request electronic evidence, while the European Preservation Order is a tool to "freeze" data quickly to prevent its deletion. The European Preservation Order is by its nature far less intrusive, and the following analysis will be more focused on the European Production Order, by virtue of which data will be transferred cross-border to law enforcement.

Orders can only be used within criminal proceedings or to enforce custodial sentences of at least four months. The Regulation specifies that European Production Orders can target four types of stored data: subscriber data, user-identifying data, traffic data and content data.[24] Less intrusive data (subscriber and user-identifying data) can be requested by a judge (including investigating judge), a court or a public prosecutor, but requests concerning more sensitive data (traffic and content) are not available for prosecutors.[25] Orders are transmitted to service providers via standardized certificates,[26] and service providers must respond within ten days (or eight hours in emergencies).[27] Providers can refuse orders only for limited reasons, such as errors or conflicting legal obligations from a third country.[28] If a service provider refuses, they must explain their reasons using a specific form.[29]

A key feature of the system that the EPOR establishes is that orders are addressed by law enforcement authorities (judges, courts or prosecutors) directly to the service providers (i.e. to their designated establishment or legal representative) bypassing – in principle – the authorities in the member state where this establishment or representative is located. This rule has one significant exception, which requires – in case of orders for traffic or content data – that such authorities are indeed informed about the request and may block or limit data transfer under specific conditions, including fundamental rights breaches. In practice, however, this limitation will arguably have limited application and in fact the main interaction will be between the authorities in the issuing state and the service provider requested to provide data.[30]

The Regulation establishes penalties for non-compliance, with potential fines of up to 2% of the provider's annual global turnover. It also requires that a "decentralised IT system" be provided in order to facilitate secure communication between authori-

[24] Article 3 (9) and (12) EPOR.

[25] Article 4 EPOR.

[26] Article 9 EPOR and Annexes I and II to the EPOR.

[27] Article 10 (1) to (4) EPOR.

[28] Article 11 (4) to (6) EPOR.

[29] Annex III to the EPOR.

[30] For the examination of the requirement of notification and the arguments about its limited practical usage, see S. Tosza, *Mutual Recognition…*

ties and service providers.[31] It already entered into force and is directly applicable in Member States' legal systems. However, it will apply only from 18 August 2026.[32] Member States have until 18 February 2026 to implement the Directive.

To complete the picture of the new solutions, the Second Protocol to the Cybercrime Convention shall also be mentioned.[33] The provisions that it introduces are, however, very limited in scope, thus it cannot be expected that as such it will be a real game-changer for the international gathering of electronic evidence. The Protocol requires – in Articles 6 and 7 – that state parties provide for possibilities of direct cooperation with service providers, although it limits this requirement to gathering of domain name registration information and subscriber information.[34] Nonetheless, one should not underestimate the impact the protocol might have long term. Due to the global impact of the Cybercrime Convention, it has a potential to facilitate change of perspective and make non-EU countries more prompt to further develop direct access to data of service providers by foreign law enforcement. In that context it is worth underlining that the Protocol has been already signed not only by most members of the Council of Europe, but also by such non-EU countries as U.S., Argentina, Morocco and Japan.[35] The years to come will show the effective impact of the Protocol, which will depend in the first place on the number of ratifications, which so far stands at two.[36]

In a nutshell, at the moment of writing the old solutions are still in place: the EIO serves as the main tool to acquire electronic evidence cross-border within the EU. The MLA system is the main instrument that has to be used for requests to non-EU providers, unless there is no obstacle for them to provide data without such a procedure (such as for non-content data requests addressed to U.S. providers). Some countries, such as Belgium, continue to apply their redefined concept of territoriality requesting cooperation from foreign providers active on its territory by means of national rules.

This system is set to end once the e-evidence package takes full effect, reshaping the process of gathering electronic evidence within the EU. This will happen only once the Directive is implemented, and the Regulation starts applying in the summer of 2026. There is, however, a number of unknowns that have to be clarified by that date for the system to be able to function and the details of the solutions provided will determine how effective the new system will be.

---

[31] Articles 19–26 EPOR.

[32] Article 34 (2) EPOR.

[33] Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, CETS no. 224.

[34] *Ibidem*.

[35] Council of Europe, *Chart of Signatures and Ratifications of Treaty 224*, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224 (access: 16.12.2024).

[36] See *ibidem*, Serbia and Japan.

Firstly, negotiations under the CLOUD Act remain one of the key open questions of the new system as without an agreement with the U.S., American providers will be in a conflict of laws if they have to comply with the European Production Order concerning content data. Complying with European Production Order in that context would automatically violate U.S. law. Secondly, while the e-evidence package addresses most aspects of the new system, several issues are left for national legislators to resolve. Thirdly, some crucial questions remain entirely unaddressed by the e-evidence package, yet they still significantly influence the ability to access data for gathering evidence in criminal proceedings. The following sections will explore these issues in greater detail.

CHALLENGES OF THE TRANSPOSITION OF THE E-EVIDENCE REGULATION

The core component of the e-evidence package is a regulation, an uncommon but not unprecedented choice for legislation related to cooperation in criminal matters.[37] This choice means that the provisions of the e-evidence Regulation became directly applicable in all EU Member States, except Denmark,[38] as soon as the regulation entered into force on 18 August 2023. However, the Regulation does not provide for an all-encompassing legal framework. Several aspects, such as the regime of sanctions and applicable remedies, are left to national legislators. In these respects, the Regulation will need to be transposed as if it were a directive. Additionally, the Regulation mandates the implementation of specific technological solutions for creating and using a decentralized IT system to securely exchange communications and data between competent authorities and service providers.

The practical usefulness and effectiveness of the e-evidence package will depend on the efforts of national legislators and the quality of the technological solutions implemented. Therefore, these aspects deserve a closer examination, which is provided in detail below.

[37] Regulation (EU) 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders (OJ EU L 303/1, 28.11.2018).

[38] In accordance with Articles 1 and 2 of Protocol No. 22 on the position of Denmark, annexed to the TEU and to the TFEU, Denmark has opted out from Title V of Part Three of the TFEU. As a result, Denmark did not take part in the adoption of the e-evidence Regulation and is not bound by it or subject to its application.

1. Sanctioning non-compliance

To ensure service providers' compliance with their duty to execute orders, the Regulation establishes a penalties regime. Yet, the definition of the pecuniary penalties applicable, as well as their implementation, is left to each Member State, which shall notify, without delay, the Commission of the rules adopted.[39] The Regulation only mandates that these sanctions be "effective, proportionate and dissuasive".[40] These provisions are to be applied "without prejudice to national laws providing for criminal penalties", thus suggesting that both administrative and criminal penalties could be imposed on service providers in certain Member States, insofar as the principle of *ne bis in idem* is respected.[41]

In addition to this general requirement, Article 15 (1) EPOR requires the Member States to ensure that pecuniary penalties of up to 2% of the total worldwide annual turnover of the service provider's preceding financial year can be impose. That is a lower threshold compared to the Digital Services Act (DSA), which provides that companies may incur fines of up to 6% of their annual worldwide turnover in case of non-compliance.[42] Similarly, the General Data Protection Regulation (GDPR) can lead to fines of up to 4% of the company's global annual turnover for more severe infringements.[43]

The provisions of sanctions in national legislations will be critical for two reasons. On the one hand, significant discrepancies between the sanctioning regimes may result in forum shopping by service providers. The latter may indeed be inclined to appoint their legal representative in a Member State where the sanctions for non-compliance are lower and non-criminal in nature.[44] In this context, it is worth noting that a comparative analysis of current Member States' legislation on law enforcement requests for data from national providers reveals significant discrepancies in the severity of sanctions. For instance, penalties in Luxembourg or

---

[39] Article 15 (1) EPOR.

[40] Criteria elaborated by the Court of Justice since the *Greek Maize* case. See judgment of the Court of 21 September 1989 in case C-68/88, *Commission of the European Communities v Hellenic Republic*, ECLI:EU:C:1989:339.

[41] V. Franssen, *Cross-border Gathering of Electronic Evidence in the EU: Toward More Direct Cooperation under the E-evidence Regulation*, [in:] *Research Handbook on EU Criminal Law (2)*, eds. M. Bergström, V. Mitsilegas, T. Quintel, [forthcoming].

[42] Article 52 of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (OJ EU L 277/1, 27.10.2022).

[43] Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (OJ EU L 119/1, 4.5.2016).

[44] V. Franssen, *The European Commission's E-evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement?*, "European Law Blog" 2018.

Germany for non-compliance with production order amounts only to a few thousand EUR.[45] However, in Belgium they may amount up to EUR 240,000,[46] and in Spain even to EUR 20,000,000.[47]

Therefore, it will be crucial to observe the extent of divergence among Member States. As noted earlier, the Regulation does little to harmonize these penalties, offering no thresholds apart from the upper threshold of up to 2%. If significant discrepancies arise, an amendment to the Regulation or a new instrument may be necessary to enforce harmonisation. Additionally, the effectiveness of individual justice systems in applying these penalties, as well as the actual penalty levels, will be essential in assessing the real risk for service providers. The Regulation provide some guidance as to the imposition of penalties in Recital 70: "When assessing in the individual case the appropriate pecuniary penalty, the competent authorities should take into account all relevant circumstances, such as the nature, gravity and duration of the breach, whether it was committed intentionally or through negligence, whether the service provider has been held responsible for similar previous breaches and the financial strength of the service provider held liable". If the levels of penalties and the practice of imposing them are significantly different, courts in different Member States will also interpret those provisions differently in terms of practical pecuniary consequences.

In additional, the e-evidence package provides penalties for non-compliance with the obligations that Member States will impose by implementing the Directive, i.e. the duty to designate establishments or nominate legal representatives. Also, in that respect, the respective provision is limited to mandate that those penalties be "effective, proportionate and dissuasive".[48]

2. Assuring effective remedies

Another aspect where the Regulation combines EU law with national rules concerns legal remedies. This remains one of the most important open questions of the new system as the Regulation only sets minimum conditions for those remedies, leaving it to each Member State to fill the details.

In particular, Article 18 EPOR states the right of any person whose data were requested via a European Production Order to effective remedies against that order.[49]

---

[45] K. Ligeti, G. Robinson, *Digital Evidence and the Cooperation of Service Providers in Luxembourg*, [in:] *The Cambridge Handbook…*, p. 361; D. Brodowski, *Digital Evidence and the Cooperation of Service Providers in Germany*, [in:] *The Cambridge Handbook…*, p. 300.

[46] S. Careel, F. Verbruggen, *Digital Evidence in Criminal Matters: Belgian Pride and Prejudice*, [in:] *The Cambridge Handbook…*, pp. 238–240.

[47] C. Cuadrado Salinas, J.C. Ortiz Pradillo, *Access to Retained Data and Cooperation of Service Providers in Criminal Investigations in Spain*, [in:] *The Cambridge Handbook…*, p. 418.

[48] Article 5 of Directive 2023/1544.

[49] Article 18 (1) EPOR.

However, such a right shall be exercised before a court in the State issuing the order "in accordance with its national law".[50] It is therefore not predefined which form those remedies should take nor when (i.e. at which stage of the criminal proceeding) they should be available, despite many instances calling for a more precise indication of the available remedies.[51] The only provision in that respect states that: "Where that person is a suspect or an accused person, such person shall have the right to effective remedies during the criminal proceedings in which the data were being used".[52] Effective remedies "shall include the possibility of challenging the legality of the measure, including its necessity and proportionality".[53]

Particular criticism has been formulated as regards the place where remedies shall be executed. In particular the fact that the Regulation does not request explicitly that there is remedy available in the enforcing state was criticised.[54] The fact that remedy would only be available in the issuing state could require a person not residing in the issuing State to travel to that state in order to exercise their right to an effective remedy in local courts or finding a suitable lawyer,[55] potentially facing considerable barriers, such as language, as well as additional costs.[56] Conversely, it has been argued that when an order concerns a person outside the issuing State, the executing State could be better positioned to provide an effective remedy.[57]

In contrast, the EIO Directive[58] has been considered as offering access to effective criminal justice remedies, as suspects and accused persons can appeal to the

[50] Article 18 (2) EPOR.

[51] See, for instance, the initiative of Germany in the negotiation process: General Secretariat of the Council, *Proposal for a Regulation of the European Parliament and of the Councilon European Production and Preservation Orders for Electronic Evidence in Criminal Matters – Compilation of Member States Comments*, 28.6.2018, https://data.consilium.europa.eu/doc/document/ST-10470-2018-REV-1/en/pdf (access: 16.12.2024), p. 11.

[52] Article 18 (1) EPOR.

[53] Article 18 (2) EPOR.

[54] In this sense, see P.G. Topalnakos, *Critical Issues in the New EU Regulation on Electronic Evidence in Criminal Proceedings*, [in:] *The Cambridge Handbook…*

[55] T. Christakis, *From Mutual Trust to the Gordian Knot of Notifications: The EU E-evidence Regulation and Directive*, [in:] *The Cambridge Handbook…*

[56] European Criminal Bar Association, *E-evidence*, https://www.ecba.org/content/index.php/working-groups/e-evidence (access: 16.12.2024); EDREDRi, *e-Evidence Compromise Blows a Hole in Fundamental Rights Safeguards*, 7.2.2023, https://edri.org/our-work/e-evidence-compromise-blows-a-hole-in-fundamental-rights-safeguards (access: 16.12.2024).

[57] S. Carrera, M. Stefan, V. Mitsilegas, *Cross-Border Data Access in Criminal Proceedings and the Future of Digital Justice: Navigating the Current Legal Framework and Exploring Ways Forward Within the EU and Across the Atlantic. Report of a CEPS and QMUL Task Force*, Brussels, October 2020, https://cdn.ceps.eu/wp-content/uploads/2020/10/TFR-Cross-Border-Data-Access.pdf (access: 16.12.2024), p. 59.

[58] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ EU L 130/1, 1.5.2014).

judicial authorities of the executing State if the production or preservation of data under an EIO is believed to have violated certain rights.[59]

How the provision on effective remedies will be implemented in practice, particularly in Member States where adherence to the rule of law has been questioned, remains to be seen.[60] It will determine the effective position of persons concerned in the context of these proceedings, and, because of that, the legitimacy of the European Production Order as a tool for transnational transfer of data.

3. Providing a decentralised IT system

Lastly, the Regulation requires that all written communications between competent authorities or between competent authorities and service providers shall take place through a decentralised IT system.[61] In principle, Member State may provide their national IT systems, which will be interconnected through interoperable access points based on the e-Codex system.[62] However, the Regulation requests the Commission to provide such a reference implementation software that shall be developed by the Commission.[63]

As this decentralized IT system is currently under development, its exact operation remains unclear. What is certain is that the correct functioning of the overall system established by the Regulation will depend on its implementation and on the ability of service providers to work with that decentralized system in an efficient and secure way.

UNRESOLVED QUESTIONS

Besides issues that the e-evidence package leaves for national legislators, a number of questions were left outside of its remit. Yet, they will significantly affect the legal and practical landscape, within which electronic evidence will be gathered and used in criminal investigations and prosecutions. The crucial ones are the questions of encryption of the data and the admissibility of electronic evidence. For the overall functioning of the judicial cooperation within the Area of Freedom, Security and

[59] *Ibidem*, p. 14.

[60] Connect on Tech, *New EU Regulation on Digital Evidence Opens Up Risk of Data Misuse*, 9.2.2024, https://www.connectontech.com/new-eu-regulation-on-digital-evidence-opens-up-risk-of-data-misuse (access: 16.12.2024).

[61] Article 19 (1) EPOR.

[62] Recital 83 EPOR; Regulation (EU) 2022/850 of the European Parliament and of the Council of 30 May 2022 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-Codex system), and amending Regulation (EU) 2018/1726 (OJ EU L 150/1, 1.6.2022).

[63] Article 22 (1) EPOR.

Justice, of high importance will be also the issue of the interaction between the European Production Order and the European Investigation Order as two tools serving to transfer evidence cross-border. These issues are analysed in turn in this chapter.

1. Encryption of the data

Encryption technologies are increasingly being adopted across both public and private sectors to safeguard privacy and prevent unauthorized access.[64] However, the widespread use of strong encryption has created significant challenges for law enforcement when seeking access to electronic evidence crucial to criminal investigations. Although electronically stored data is often vital to these cases, encryption can make accessing such evidence exceptionally difficult, if not practically impossible. This challenge is further compounded by the rapid advancement of encryption technology and the growing diversity of its applications.[65] Electronic devices and applications are now routinely encrypting stored data by default, and a rising number of communication channels are protected with end-to-end encryption.[66] These measures ensure that only the communicating parties can decrypt and access the content. In result third parties, including the service providers, are technically prevented from accessing the information necessary for criminal investigations.[67] The outcome of this phenomenon is that despite being equipped with a warrant or court order law enforcement is increasingly restricted in their capacity to access crucial evidence. This challenge is known as the "going dark" problem.[68]

Given how acute and how complex the problem remains, it is at the same time striking and not surprising that the Regulation omits to address the problem of encryption, which remains one of the "elephants in the room" for the gathering of electronic evidence.[69] It merely states in Recital 20 EPOR that its application "should not affect the use of encryption by service providers or their users" and that the Regulation does not "lay down any obligation for service providers to decrypt data".[70]

---

[64] O.L. van Daalen, *The Right to Encryption: Privacy as Preventing Unlawful Access*, "Computer Law & Security Review" 2023, vol. 49.

[65] For a description of modern encryption technologies see C. Delpech de Saint Guilhem, *On Encryption Technologies and Potential Solutions for Lawful Access*, [in:] *The Cambridge Handbook…*

[66] Europol, *First Report on Encryption by the EU Innovation Hub for Internal Security*, 2024, https://www.eurojust.europa.eu/sites/default/files/assets/eu-innovation-hub-first-report-on-encryption.pdf (access: 16.12.2024), p. 43.

[67] C. Delpech de Saint Guilhem, *op. cit*.

[68] I. Walden, *'The Sky is Falling!' – Responses to the 'Going Dark' Problem*, "Computer Law & Security Review" 2018, vol. 34, pp. 901–907; T. Moraes, *Sparkling Lights in the Going Dark: Legal Safeguards for Law Enforcement's Encryption Circumvention Measures*, "European Data Protection Law Review" 2020, vol. 6(1), pp. 41–55.

[69] V. Franssen, *Cross-border…*

[70] Recital 20 EPOR.

Service providers should provide or preserve data requested by means of a European Production Order or a European Preservation Order "regardless of whether they are encrypted or not".[71] In this regard, the Regulation does not directly provide law enforcement authorities with tools to address the challenges encryption poses in criminal investigations.

In some instances, however, national law may play a role, as certain Member States already have general legal provisions in place to assist law enforcement authorities in tackling the encryption challenge.[72] That is the case, for instance, of national legislation requiring service providers to produce data in a legible format, such as in Ireland.[73] Likewise, France has long established a criminal offence for individuals refusing to communicate "the secret decryption method of a cryptographic device likely to have been used to prepare, facilitate or commit a crime or misdemeanour".[74] According to the French High Court, such decryption methods include the code required to unlock a phone.[75] In contrast, in Poland, the investigated person has no obligation to disclose such a code, as doing so would contravene their right to silence and to not incriminate themselves.[76]

2. Admissibility of evidence acquired through the European Production Order

The e-evidence Regulation does not provide any rules, which concern admissibility of electronic evidence gathered through the Regulation. The only provision of the e-evidence Regulation that might have an impact on the admissibility – or rather inadmissibility – of evidence is contained in Article 20 which states that electronic evidence shall not "be considered inadmissible in the context of cross-border judicial procedures (…) solely on the ground that they are in electronic form". This provision contains a sort of non-discrimination clause concerning the electronic form of the evidence, but does not say anything else as regards admissibility of electronic evidence gathered through the European Production Order.

Furthermore, Article 18 (5) EPOR merely that "without prejudice to national procedural rules, the issuing State and any other Member State to which electronic evidence has been transmitted under this Regulation shall ensure that the rights

[71] *Ibidem*.

[72] Europol, *op. cit.*, p. 49.

[73] See T.J. McIntyre, M.H. Murphy, *Accessing Digital Evidence in Criminal Matters: An Inadequate Irish Legal Framework*, [in:] *The Cambridge Handbook…*

[74] Article 434-15-2 of the French Criminal Code.

[75] Cour de Cassation, Assemblée plénière, 7 novembre 2022, no. 21-83146, no. 21-83146.

[76] W. Zontek, *„Mój smartfon to ja". Hasła i zabezpieczenia biometryczne a reguły procesowe w XXI wieku*, [in:] *Prawo karne gospodarcze. Księga jubileuszowa profesora Zbigniewa Ćwiąkalskiego*, eds. P. Kardas, M. Małecki, W. Wróbel, Kraków 2023.

of defence and fairness of the proceedings are respected when assessing evidence obtained through the European Production Order". It results from this rule that it is for the Member States to decide what sort of consequences a violation of procedural rules concerning the European Production Order will have.[77] For instance, when data is obtained through a European Production Order issued by an authority lacking the competence to do so, and the service providers do not oppose to its execution, the usability at trial of this unlawfully obtained electronic evidence will depend on national rules on the admissibility of evidence of the issuing Member State.[78] While in several EU legal systems, illegal evidence will not be automatically excluded (admissible under a balancing test), in a few jurisdictions, any illegality will render the evidence inadmissible.[79] Therefore, not only European legislation on the matter is *de facto* inexistent, but national rules on admissibility of criminal evidence still diverge significantly among Member States.[80]

The e-evidence Regulation offers a unique model – in comparison to the European Arrest Warrant or the European Investigation Order "traditional" one – of mutual recognition, which is based on direct cross-border interaction between law enforcement and a private party obliged to produce evidence.[81] How much this particularity will have an impact on the practice of the European Production Order will have to be seen once the new model starts functioning in practice.

This feature potentially undermines, nonetheless, not only the effectiveness of the prosecution but also the rights of the defence. However, Member States have traditionally resisted addressing the issue of admissibility of evidence at the EU level, even though a specific legal basis for doing so exists in the Treaties. In fact, Article 82 (2) TFEU expressly mentions the possibility to adopt EU law on "mutual admissibility of evidence between Member States" to the extent "necessary to facilitate mutual recognition of judgments and judicial decisions and police and judicial cooperation in criminal matters having a cross-border dimension". Against this backdrop, the European Law Institute (ELI) has recently presented a Proposal for a Directive on mutual admissibility of evidence and electronic evidence in criminal proceedings, which also includes a specific part setting out concrete rules on electronic evidence.[82]

---

[77] V. Franssen, *Cross-border…*

[78] Eadem, *The European…*

[79] S.C. Thaman, *Balancing Truth Against Human Rights: A Theory of Modern Exclusionary Rules*, [in:] *Exclusionary Rules in Comparative Law*, ed. S.C. Thaman, Cham 2013.

[80] G. Lasagni, *Admissibility of Digital Evidence*, [in:] *The Cambridge Handbook…*

[81] S. 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*, "New Journal of European Criminal Law" 2020, vol. 11(2), pp. 161–183.

[82] European Law Institute, *ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings:*

Lastly, an important reflection on the admissibility of evidence at the European level was triggered by the proceedings resulting from the EncroChat investigations. Several courts have ruled in favour of usability of that evidence in domestic criminal proceedings.[83] Notably, the Italian Supreme Court of Cassation based itself on the presumption that the interception was legally carried out and argued that evidence thus acquired via an EIO could be used without any further scrutiny.[84] The Court further held that the defence's inability to access the algorithms used by foreign authorities to decrypt communications does not represent, in principle, a violation of fundamental rights.[85] However, departing from the Opinion of the Advocate General who emphasised that admissibility of evidence is a matter of national legislation,[86] the Court did not shy away to pronounce itself on the issue of admissibility and, based on Article 14 (7) of the EIO Directive, stated that evidence "must be excluded" from the criminal proceedings if the defendant is not in a position to comment effectively on the way it was collected.[87]

3. Relationship between the European Production Order and the European Investigation Order

Another question that is not directly resolved by the e-evidence Regulation concerns the relationship between the European Production Order and the European Investigation Order (EIO). As said, at this point the EIO is the main instrument through which enforcement authorities may request data transnationally within the EU.

The EIO introduced by the EIO Directive of 2014 and with the transposition date of May 2017, has been since then the overall instrument of gathering evidence from a different Member State (with the exception of Ireland and Denmark). Once the European Production Order starts to be operational we will be able to talk

---

Draft Legislative Proposal of the European Law Institute, 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 (access: 16.12.2024). A study, on which this proposal is based, was published as L. Bachmaier Winter, F. Salimi (eds.), *Admissibility of Evidence in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair Trial Rights*, Oxford 2024.

[83] Europol, *op. cit.*, p. 5. Namely, Italy, Germany, France and the Netherlands.

[84] G. Di Paolo, *Admissibility of E-evidence, Transnational E-evidence and Fair-Trial Rights in Italy*, [in:] *Admissibility of Evidence in EU Cross-Border Criminal Proceedings…*, p. 87.

[85] M. Daniele, *Le sentenze "gemelle" delle Sezioni Unite sui criptofonini*, "Sistema penale", 17 July 2024, https://www.sistemapenale.it/it/scheda/daniele-le-sentenze-gemelle-delle-sezioni-unite-sui-criptofonini#_ftnref41 (access: 16.12.2024).

[86] T. Wahl, *AG: EncroChat Data Can, in Principle, Be Used in Criminal Proceedings*, "Eucrim" 2024, no. 3.

[87] Judgment of the Court (Grand Chamber) of 30 April 2024 in case C-670/22, *Criminal proceedings against M.N. (EncroChat)*, ECLI:EU:C:2024:372, pp. 130–131.

about the duality of instruments of transnational cooperation as regards gathering of evidence with a general instrument being the EIO, which will be applicable in particular to live data transmission and data to be gathered from other sources than service providers as well as a special regime for stored data in the possession of service providers, i.e. the European Production Order.[88]

It is very clear that the European Production Order is a quicker and easier instrument to apply.[89] Besides their resemblances – both instruments are based on mutual recognition – the dynamics of cooperation are fundamentally different. While the EIO is based on the interaction between public authorities in two Member States, the e-evidence Regulation has opted for the almost complete elimination of a public authorities' intervention in the State where the order is sent. That authority would only intervene if there were a need to enforce the order or in case it decided to react to the notification of Article 8 EPOR. Hence, one can easily expect that the European Production Order may become the favourite instrument of law enforcement due to lesser procedural checks built into its system.

Yet, it does not mean that the access to data is a less intrusive measure than those that will be governed still by the EIO. Nowadays, for many people the content of an email account contains much more privacy sensitive information than what can be found in their homes during a search. It remains to be seen once the European Production Order becomes operational how the balance between these two instruments will be established and what systemic consequences in practice the application of the EPOR will have.

CONCLUSIONS

As the above analysis demonstrates, despite the adoption of the e-evidence package and despite the fact that its main component is a directly applicable regulation, there remains a number of tasks for national legislators and unsolved problems. National legislators need to provide for the sanctioning system as well as assure effective remedies and the level of discrepancies between the Member States in that respect will be crucial, as will be the fact where the major providers declare their seats. While the design of the new system of cross-border gathering of electronic evidence in the EU, based in principle on direct cross-border requests to service providers active in the EU is set, its success significantly depends on the outcome of the negotiations with the U.S. concerning the CLOUD Act. Furthermore,

[88] See the analysis of the interaction between these instruments and potential systemic consequences of this duality: S. Tosza, *All Evidence Is Equal…* Although the article was written examining the e-evidence proposal in an earlier version, the overall conclusion as to that duality remains valid.

[89] In detail the comparison between EIO and the European Production Order, see *ibidem*, pp. 177–182.

the success of the e-evidence package depends on technical capacities to safely transfer the data (question of a decentralised IT system) and to having access to its content (problem of encryption).

A crucial issue, which analysis goes beyond the scope of this article, is data retention. In simple terms, if the service providers do not have the data (anymore), the requests will be futile. However, the Data Retention Directive, and with it the EU-wide data retention duties, were invalidated by the *Digital Rights Ireland* judgment.[90] Since then it a subject of intensive debate whether and to what extent data retention obligations can be provided in accordance with the Charter of Fundamental Rights of the EU, while different such obligations may be found in national legal systems.[91]

These are not the only missing pieces or unresolved problems. For instance, the CLOUD Act agreement would solve only the conflicts of laws with the U.S. However, providers established in third countries may be subject to similar constraints as the U.S. ones and once they have sufficient usage by the EU customers they fall under the obligations of the e-evidence package. This might concern, for instance, persons belonging to significant minorities in the EU, e.g. the Turkish one, who might have a preference to use services offered by a Turkish provider. Such a service, even based entirely in Turkey, would fall under the obligations of the e-evidence package.

The e-evidence package remains a controversial piece of legislation due to the risks for fundamental rights, especially the right to privacy, and in particular because of the elimination of the control of the executing/enforcing state in most cases, which is a standard for other mutual recognition instruments. This article did not examine these issues in detail, which were subject to extensive examination, including by the author.[92] However, one has to admit that the adoption of the e-evidence package was a major breakthrough. Despite the criticism it must be acknowledged that the EU addressed a significant challenge posed by the borderless nature of cyberspace and digital capitalism, which hampers effective investigation and prosecution. Whether the e-evidence package will be a success depends still on significant efforts to assure its effectiveness, technological robustness of its execution as well as assurance that violations of fundamental rights can be adequately remedied.

---

[90] Judgment of the Court (Grand Chamber) of 8 April 2014 in joined cases C-293/12 and C-594/12, *Digital Rights Ireland and others*, ECLI:EU:C:2014:238.

[91] See comparatively S. Tosza, V. Franssen, *A Comparative Analysis of National Law and Practices: Unravelling Differences in Views of EU-Wide Solutions*, [in:] *The Cambridge Handbook…*, pp. 431–434.

[92] In that respect, see in particular S. Tosza, *Mutual Recognition…*; idem, *All Evidence Is Equal…*

REFERENCES

Literature

Bachmaier Winter L., Salimi F. (eds.), *Admissibility of Evidence in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair Trial Rights*, Oxford 2024, **DOI: https://doi.org/10.5040/9781509972029**.

Bilgiç S., *Digital Evidence Collection in Turkey*, [in:] *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, eds. V. Franssen, S. Tosza, 2025 [forthcoming].

Brodowski D., *Digital Evidence and the Cooperation of Service Providers in Germany*, [in:] *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, eds. V. Franssen, S. Tosza, 2025 [forthcoming].

Careel S., Verbruggen F., *Digital Evidence in Criminal Matters: Belgian Pride and Prejudice*, [in:] *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, eds. V. Franssen, S. Tosza, 2025 [forthcoming].

Christakis T., *From Mutual Trust to the Gordian Knot of Notifications: The EU E-evidence Regulation and Directive*, [in:] *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, eds. V. Franssen, S. Tosza, 2025 [forthcoming].

Cuadrado Salinas C., Ortiz Pradillo J.C., *Access to Retained Data and Cooperation of Service Providers in Criminal Investigations in Spain*, [in:] *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, eds. V. Franssen, S. Tosza, 2025 [forthcoming].

Daalen O.L. van, *The Right to Encryption: Privacy as Preventing Unlawful Access*, "Computer Law & Security Review" 2023, vol. 49, **DOI: https://doi.org/10.1016/j.clsr.2023.105804**.

Daskal J., *The Un-territoriality of Data*, "The Yale Law Journal" 2015, vol. 125.

Daskal J., *Unpacking the CLOUD Act*, "Eucrim" 2018, no. 4, **DOI: https://doi.org/10.30709/eucrim-2018-022**.

Delpech de Saint Guilhem C., *On Encryption Technologies and Potential Solutions for Lawful Access*, [in:] *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, eds. V. Franssen, S. Tosza, 2025 [forthcoming].

Di Paolo G., *Admissibility of E-evidence, Transnational E-evidence and Fair-Trial Rights in Italy*, [in:] *Admissibility of Evidence in EU Cross-Border Criminal Proceedings: Electronic Evidence, Efficiency and Fair Trial Rights*, eds. L. Bachmaier Winter, F. Salimi, Oxford 2024, **DOI: https://doi.org/10.5040/9781509972029.ch-005**.

Filatova M., Kostyleva O., Alekseeva T., *Cooperation of Service Providers in Criminal Investigations in the Russian Federation*, [in:] *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, eds. V. Franssen, S. Tosza, 2025 [forthcoming].

Franssen V., *Cross-border Gathering of Electronic Evidence in the EU: Toward More Direct Cooperation under the E-evidence Regulation*, [in:] *Research Handbook on EU Criminal Law (2)*, eds. M. Bergström, V. Mitsilegas, T. Quintel, [forthcoming].

Franssen V., *The Belgian Internet Investigatory Powers Act – A Model to Pursue at European Level?*, "European Data Protection Law Review" 2017, vol. 3(4), **DOI: https://doi.org/10.21552/edpl/2017/4/18**.

Franssen V., *The European Commission's E-evidence Proposal: Toward an EU-wide Obligation for Service Providers to Cooperate with Law Enforcement?*, "European Law Blog" 2018, **DOI: https://doi.org/10.21428/9885764c.8139cb70**.

Franssen V., Tosza S. (eds.), *The Cambridge Handbook of Digital Evidence in Criminal Matters, Cambridge University Press*, 2025 [forthcoming].

Kusak M., *Dostęp do danych elektronicznych dotyczących treści w postępowaniu karnym – wyzwania krajowe i międzynarodowe*, "Gdańskie Studia Prawnicze" 2024, no. 2, **DOI: https://doi.org/10.26881/gsp.2024.2.05**.

Lasagni G., *Admissibility of Digital Evidence*, [in:] *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, eds. V. Franssen, S. Tosza, 2025 [forthcoming].

Ligeti K., Robinson G., *Digital Evidence and the Cooperation of Service Providers in Luxembourg*, [in:] *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, eds. V. Franssen, S. Tosza, 2025 [forthcoming].

McIntyre T.J., Murphy M.H., *Accessing Digital Evidence in Criminal Matters: An Inadequate Irish Legal Framework*, [in:] *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, eds. V. Franssen, S. Tosza, 2025 [forthcoming].

Mitsilegas V., *The Privatisation of Mutual Trust in Europe's Area of Criminal Justice: The Case of E-evidence*, "Maastricht Journal of European and Comparative Law" 2018, vol. 25(3), **DOI: https://doi.org/10.1177/1023263X18792240**.

Moraes T., *Sparkling Lights in the Going Dark: Legal Safeguards for Law Enforcement's Encryption Circumvention Measures*, "European Data Protection Law Review" 2020, vol. 6(1), **DOI: https://doi.org/10.21552/edpl/2020/1/7**.

Sieber U., Neubert C., *Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty*, "Max Planck Yearbook of United Nations Law Online" 2017, vol. 20, **DOI: https://doi.org/10.1163/13894633_02001010**.

Thaman S.C., *Balancing Truth Against Human Rights: A Theory of Modern Exclusionary Rules*, [in:] *Exclusionary Rules in Comparative Law*, ed. S.C. Thaman, Cham 2013.

Topalnakos P.G., *Critical Issues in the New EU Regulation on Electronic Evidence in Criminal Proceedings*, [in:] *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, eds. V. Franssen, S. Tosza, 2025 [forthcoming].

Tosza S., *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*, "New Journal of European Criminal Law" 2020, vol. 11(2), **DOI: https://doi.org/10.1177/2032284420919802**.

Tosza S., *Internet Service Providers as Law Enforcers and Adjudicators: A Public Role of Private Actors*, "Computer Law & Security Review" 2021, vol. 43, **DOI: https://doi.org/10.1016/j.clsr.2021.105614**.

Tosza S., *Mutual Recognition by Private Actors in Criminal Justice? E-evidence Regulation and Service Providers as the New Guardians of Fundamental Rights*, "Common Market Law Review" 2024, vol. 61(1), **DOI: https://doi.org/10.54648/COLA2024005**.

Tosza S., *The E-evidence Package Is Adopted: End of a Saga or Beginning of a New One?*, "European Data Protection Law Review" 2023, vol. 9.

Tosza S., *W poszukiwaniu dowodów elektronicznych – europejski nakaz wydania dowodów elektronicznych oraz inne narzędzia międzynarodowego pozyskiwania danych dla potrzeb postępowania karnego*, "Gdańskie Studia Prawnicze" 2024, no. 2, **DOI: https://doi.org/10.26881/gsp.2024.2.03**.

Tosza S., FranssenV., *A Comparative Analysis of National Law and Practices: Unravelling Differences in Views of EU-Wide Solutions*, [in:] *The Cambridge Handbook of Digital Evidence in Criminal Investigations*, eds. V. Franssen, S. Tosza, 2025 [forthcoming].

Wahl T., *AG: EncroChat Data Can, in Principle, Be Used in Criminal Proceedings*, "Eucrim" 2024, no. 3.

Walden I., *'The Sky is Falling!' – Responses to the 'Going Dark' Problem*, "Computer Law & Security Review" 2018, vol. 34, **DOI: https://doi.org/10.1016/j.clsr.2018.05.013**.

Zontek W., *„Mój smartfon to ja". Hasła i zabezpieczenia biometryczne a reguły procesowe w XXI wieku*, [in:] *Prawo karne gospodarcze. Księga jubileuszowa profesora Zbigniewa Ćwiąkalskiego*, eds. P. Kardas, M. Małecki, W. Wróbel, Kraków 2023.

Online sources

Agreement between the Government of Australia and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, https://www.home-affairs.gov.au/nat-security/files/cloud-act-agreement-signed.pdf (access: 16.12.2024).

Böse M., *An Assessment of the Commission's Proposals on Electronic Evidence*, 2018, https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf (access: 16.12.2024).

Carrera S., Stefan M., Mitsilegas V., *Cross-Border Data Access in Criminal Proceedings and the Future of Digital Justice: Navigating the Current Legal Framework and Exploring Ways Forward Within the EU and Across the Atlantic. Report of a CEPS and QMUL Task Force*, Brussels, October 2020, https://cdn.ceps.eu/wp-content/uploads/2020/10/TFR-Cross-Border-Data-Access.pdf (access: 16.12.2024).

Clarke R.A., Morell M.J., Stone G.R., Sunstein C.R., Swire P., *Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies*, 12.12.2013, https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (access: 16.12.2024).

Connect on Tech, *New EU Regulation on Digital Evidence Opens Up Risk of Data Misuse*, 9.2.2024, https://www.connectontech.com/new-eu-regulation-on-digital-evidence-opens-up-risk-of-data-misuse (access: 16.12.2024).

Council of Europe, *Chart of Signatures and Ratifications of Treaty 224*, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224 (access: 16.12.2024).

Daniele M., *Le sentenze "gemelle" delle Sezioni Unite sui criptofonini*, "Sistema penale", 17 July 2024, https://www.sistemapenale.it/it/scheda/daniele-le-sentenze-gemelle-delle-sezioni-unite-sui-criptofonini#_ftnref41 (access: 16.12.2024).

EDRi, *e-Evidence Compromise Blows a Hole in Fundamental Rights Safeguards*, 7.2.2023, https://edri.org/our-work/e-evidence-compromise-blows-a-hole-in-fundamental-rights-safeguards (access: 16.12.2024).

European Commission, *Non-Paper: Progress Report Following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace*, Brussels, 7.12.2016, https://data.consilium.europa.eu/doc/document/ST-15072-2016-REV-1/en/pdf (access: 16.12.2024).

European Commission, *EU-U.S. Announcement on the Resumption of Negotiations on an EU-U.S. Agreement to Facilitate Access to Electronic Evidence in Criminal Investigations*, 2.3.2023, https://commission.europa.eu/news/eu-us-announcement-resumption-negotiations-eu-us-agreement-facilitate-access-electronic-evidence-2023-03-02_en (access: 16.12.2024).

European Criminal Bar Association, *E-evidence*, https://www.ecba.org/content/index.php/working-groups/e-evidence (access: 16.12.2024).

European Law Institute, *ELI Proposal for a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings: Draft Legislative Proposal of the European Law Institute*, 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 (access: 16.12.2024).

Europol, *First Report on Encryption by the EU Innovation Hub for Internal Security*, 2024, https://www.eurojust.europa.eu/sites/default/files/assets/eu-innovation-hub-first-report-on-encryption.pdf (access: 16.12.2024).

General Secretariat of the Council, *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters – Compilation of Member States Comments*, 28.6.2018, https://data.consilium.europa.eu/doc/document/ST-10470-2018-REV-1/en/pdf (access: 16.12.2024).

U.S. Department of Justice, Cloud Act Agreement between the Governments of the U.S., United Kingdom of Great Britain and Northern Ireland, https://www.justice.gov/criminal/criminal-oia/cloud-act-agreement-between-governments-us-united-kingdom-great-britain-and-northern#:~:-text=The%20Agreement%20provides%20an%20efficient,consistent%20with%20its%20law%20 and (access: 16.12.2024).

Woods K., Swire P., *The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems*, 6.2.2018, https://www.lawfaremedia.org/article/cloud-act-welcome-legislative-fix-cross-border-data-problems (access: 16.12.2024).

Legal acts

Clarifying Lawful Overseas Use of Data Act – CLOUD Act, S. 2383, 115th Cong. § 2(1)–(2) (2018) (codified at 18 U.S.C. §§ 2713, 2523 (2018).

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ EU L 130/1, 1.5.2014).

Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings (OJ EU L 191/181, 28.7.2023).

French Criminal Code.

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, Strasbourg,17.4.2018, COM/2018/226 final.

Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, Strasbourg, 17.4.2018, COM/2018/225 final.

Regulation (EU) 2016/679 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 and on the free movement of such data, and repealing Directive 95/46/EC (OJ EU L 119/1, 4.5.2016).

Regulation (EU) 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders (OJ EU L 303/1, 28.11.2018).

Regulation (EU) 2022/850 of the European Parliament and of the Council of 30 May 2022 on a computerised system for the cross-border electronic exchange of data in the area of judicial cooperation in civil and criminal matters (e-Codex system), and amending Regulation (EU) 2018/1726 (OJ EU L 150/1, 1.6.2022).

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (OJ EU L 277/1, 27.10.2022).

Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (OJ EU L 191/118, 28.7.2023).

Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, CETS no. 224.

Case law

Cour de Cassation, Assemblée plénière, 7 novembre 2022, no. 21-83146, no. 21-83146.

Decision of the U.S. Court of Appeals – Second Circuit of 14 July 2016, *Microsoft Corp. v. United States* (so-called Microsoft Ireland Case), 829 F.3d 197.

Judgment of the Court of 21 September 1989 in case C-68/88, *Commission of the European Communities v Hellenic Republic*, ECLI:EU:C:1989:339.
Judgment of the Court (Grand Chamber) of 8 April 2014 in joined cases C-293/12 and C-594/12, *Digital Rights Ireland and others*, ECLI:EU:C:2014:238.
Judgment of the Court (Grand Chamber) of 30 April 2024 in case C-670/22, *Criminal proceedings against M.N. (EncroChat)*, ECLI:EU:C:2024:372.
Judgment of the Permanent Court of International Justice on 7 September 1927, *SS Lotus (Fr. v. Turk.)*, Publications of the Permanent Court of International Justice, Series A.-No. 70.

ABSTRAKT

W dniu 12 lipca 2023 r. Unia Europejska przyjęła po pięciu długich latach negocjacji pakiet dotyczący dowodów elektronicznych. Pakiet ten wprowadza nowy model wzajemnego uznawania w celu zapewnienia transgranicznego dostępu do danych na potrzeby postępowania karnego. Ten nowy model ma zapewnić skuteczniejszy sposób pozyskiwania danych od usługodawców działających na terenie Unii Europejskiej, lecz zlokalizowanych poza granicami państwa prowadzącego postępowanie. Będzie to miało miejsce poprzez umożliwienie bezpośredniego żądania danych od usługodawców z pominięciem organów w państwach członkowskich, w których ustawodawca jest zlokalizowany. Usługodawcy będą zobowiązani do wyznaczenia co najmniej jednego zakładu lub przedstawiciela uprawnionego do przyjmowania nakazów wydania dowodów elektronicznych oraz sprawnego reagowania na te nakazy. Chociaż przyjęcie pakietu w sprawie dowodów elektronicznych stanowi niewątpliwie ważny krok na drodze do rozwiązania problemu dostępu do danych na potrzeby postępowania karnego, jego skuteczność i praktyczne zastosowanie zależą od kilku zasadniczych zagadnień, które pakiet pozostawia w gestii państw członkowskich lub w ogóle pomija, a także od osiągnięcia porozumienia ze Stanami Zjednoczonymi w ramach tzw. *CLOUD Act*. Artykuł ma na celu przedstawienie obecnej sytuacji prawnej dotyczącej transgranicznego dostępu do dowodów elektronicznych, przeanalizowanie owych nierozwiązanych zagadnień oraz ocenę ich wpływu na ostateczny kształt systemu dostępu do dowodów elektronicznych w ramach Unii Europejskiej.

Słowa kluczowe: dowody elektroniczne; europejski nakaz wydania dowodów elektronicznych; dostawcy usług internetowych; szyfrowanie; dopuszczalność dowodów; europejski nakaz dochodzeniowy

UMCS
WYDAWNICTWO