

Marcin Warchoł
University of Warsaw
<https://orcid.org/0000-0003-1253-7350>
marcinwarchol@wpia.uw.edu.pl

Access to Electronic Evidence in Criminal Proceedings in the Light of European Union Law

Dostęp do dowodów elektronicznych w sprawach karnych w świetle prawa Unii Europejskiej

Abstract

The new EU regulation on electronic evidence in criminal proceedings aims to strengthen cross-border access to such evidence. 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 provides that the relevant authorities have access to stored data, regardless of its location. Using the production order, the judicial authority of one Member State can directly request access to electronic evidence from a service provider established or represented in another Member State. The e-evidence package is designed to facilitate and accelerate the ability of law enforcement and judicial authorities to obtain the electronic evidence necessary for investigations and potential prosecution. The package consists of a Regulation and a Directive.

However, the speed and effectiveness of access to electronic evidence comes at the expense of the principles of sovereignty, mutual cooperation, and the protection of civil rights and freedoms. Direct cooperation between the issuing state and a private service provider concerning the data of citizens from other Member States violates Article 82 TFEU. The mutual recognition of court decisions in criminal matters is one of the fundamental principles in the area of freedom, security, and justice.

This leads to circumventing the traditional principle of verification by the judicial authorities of the executing state. Moreover, these solutions eliminate the requirement of dual criminality, which could lead to the collection of data concerning acts that may not be punishable in the executing state. Additionally, the lack of the principle of specialty allows for the arbitrary and discretionary use of the collected evidence, not necessarily in line with the original purpose for which it was obtained. Finally, individuals' rights to privacy and data protection are threatened. Furthermore, there are no clear provisions for legal protection in the executing state.

Keywords: electronic evidence, European Production Order, mutual recognition of judicial decisions, personal data protection, state sovereignty

Streszczenie

Nowa unijna regulacja o dowodach elektronicznych w postępowaniach karnych przewiduje wzmocnienie transgranicznego dostępu do nich. Rozporządzenie o nakazie wydania i nakazie zabezpieczenia dowodów elektronicznych stanowi, że odpowiednie organy mają dostęp do przechowywanych danych, bez względu na miejsce ich przechowywania. Korzystając z nakazu wydania dowodów, organ sądowy jednego państwa członkowskiego może wystąpić o dostęp do dowodu elektronicznego bezpośrednio do dostawcy usług mającego siedzibę lub przedstawicielstwo w innym państwie członkowskim. Pakiet dowodów elektronicznych (e-evidence) ma za zadanie ułatwić i przyspieszyć organom ścigania i instytucjom sądowym uzyskiwanie dowodów elektronicznych niezbędnych do przeprowadzenia śledztwa i ewentualnego oskarżenia. Pakiet składa się z Rozporządzenia i Dyrektywy. Przedmiotem opracowania jest rozporządzenie.

Niestety jednak szybkość i skuteczność dostępu do dowodów elektronicznych odbywa się kosztem zasady suwerenności, wzajemnej współpracy oraz ochrony praw i wolności obywatelskich. Bezpośrednia współpraca między państwem wydającym, a prywatnym usługodawcą w kwestii danych obywateli z innych państw członkowskich narusza art. 82 TFUE. Wzajemne uznawanie orzeczeń sądowych w sprawach karnych jest jedną z głównych zasad w obszarze wolności, bezpieczeństwa i sprawiedliwości.

Prowadzi to do obejścia tradycyjnej zasady weryfikacji przez organy sądowe państwa wykonującego. Ponadto, rozwiązania te eliminują

wymóg podwójnej karalności. Może to prowadzić do zbierania danych za zachowania, które nie muszą być karane w państwie wykonującym. Dodatkowo brak zasady specjalności pozwala na dowolne i uznaniowe wykorzystanie zebranych dowodów niekoniecznie zgodnie z celem ich pozyskania. Wreszcie zagrożone są prawa jednostek do prywatności i ochrony danych osobowych. Co więcej, brak jest wyraźnych rozwiązań dla ochrony prawnej w państwie wykonującym.

Słowa kluczowe: dowody elektroniczne, europejski nakaz wydania, wzajemne uznawanie orzeczeń sądowych, ochrona danych osobowych, suwerenność państwa

The new EU regulation on electronic evidence in criminal proceedings aims to strengthen cross-border access to such evidence¹. The Regulation on European Production Orders and European Preservation Orders for electronic evidence provides that competent authorities should have access to stored data regardless of where the data are located. By using a Production Order, a judicial authority in one Member State may request access to electronic evidence directly from a service provider established or represented in another Member State. The service provider will be required to respond within 10 days and, in exceptional circumstances, within 8 hours². In more than half of criminal cases, there is a need to execute cross-border requests for access to electronic evidence such as texts, emails, or messaging applications³.

The e-evidence package is intended to facilitate and accelerate the acquisition of electronic evidence necessary for conducting investigations and possible prosecutions by law enforcement authorities and judicial institutions. The package consists of a Regulation and a Directive. Under this mechanism, judicial authorities in one Member State will be able to obtain electronic evidence (such as emails, texts, or messages exchanged through applications, as well as information enabling the identification of a perpetrator at an early stage) directly from a service

¹ 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, Official Journal of the European Union, L 191/118.

² *E-evidence – cross-border access to electronic evidence*, „Consilium”, <https://www.consilium.europa.eu/pl/policies/e-evidence/> [accessed: 1 July 2026].

³ *E-evidence – cross-border access to electronic evidence*, „European Commission”, https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en [accessed: 1 July 2026].

provider or its legal representative in another Member State. The provider will be obliged to respond within 10 working days and, in urgent cases, within 8 hours (as compared to up to 120 days under the European Investigation Order procedure or an average of 10 months under mutual legal assistance procedures).

Judicial authorities in one Member State may also require a service provider or its legal representative in another Member State to preserve specific data in connection with a subsequent request for disclosure through mutual legal assistance, a European Investigation Order, or a European Production Order. These proposals are intended to simplify and expedite procedures related to access to electronic evidence in cross-border criminal cases⁴. The Preservation Order obliges the service provider not to delete electronic evidence until the request for a Production Order has been examined.

However, since the initiation of work on these solutions, there has been no shortage of criticism. It has been emphasized that they raise serious concerns regarding respect for the right to privacy and fundamental rights⁵.

First, direct cooperation is introduced between the issuing State and a private service provider concerning the data of citizens of other Member States. This is difficult to reconcile with Article 82 of the Treaty on the Functioning of the European Union (TFEU). Mutual recognition of judicial decisions in criminal matters is one of the fundamental principles

⁴ The European Commission justified these solutions by emphasizing the growing need for rapid and effective cross-border access to electronic evidence in criminal investigations. According to the Commission, more than half of all criminal investigations within the European Union involve requests for access to electronic evidence, such as emails, text messages, or data from messaging applications. Existing mechanisms, including mutual legal assistance procedures and the European Investigation Order, were considered excessively slow and inefficient in the digital era. The Commission argued that the e-evidence package was intended to facilitate and accelerate access to electronic evidence for law enforcement and judicial authorities, while simultaneously ensuring safeguards for fundamental rights, including the protection of personal data and access to effective legal remedies. The new framework was also presented as a means of providing greater legal certainty for service providers operating across the European Union and of ensuring uniform obligations for providers established both within and outside the EU. Furthermore, the Commission stressed that the new rules would improve judicial cooperation in combating serious crime and terrorism, particularly in situations where electronic evidence is stored in another Member State or outside the European Union. According to the Commission, direct cooperation between judicial authorities and service providers was necessary to prevent the loss of volatile electronic data and to adapt criminal justice mechanisms to technological developments. See *E-evidence – cross-border access to electronic evidence*, „European Commission”, https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en [accessed: 1 July 2026].

⁵ P. Topalnakos, *Critical Issues in the New EU Regulation on Electronic Evidence in Criminal Proceedings*, “eucrim” 2023, nr 2, p. 201.

in the area of freedom, security, and justice. The application of this principle focuses primarily on the effectiveness and recognition of foreign judicial decisions as domestic ones⁶.

Moreover, this leads to circumvention of the traditional principle of verification by judicial authorities of the executing State. Second, these solutions eliminate the requirement of double criminality for certain categories of electronic evidence. This may result in the collection of data concerning conduct that is not criminalized in the executing State⁷. Furthermore, the absence of the principle of speciality allows collected evidence to be used freely, not necessarily in accordance with the purpose for which it was obtained. Third, individuals' rights to privacy and protection of personal data are endangered because the European Preservation Order extends beyond the purpose of legal remedies. Furthermore, the lack of clear legal protection mechanisms in the executing State threatens the effectiveness of such remedies⁸.

Meanwhile, there is a need to strike a balance between the requirement for enhanced cooperation and the protection of fundamental freedoms. Legal solutions should be implemented to ensure effective review of the legality and justification of undertaken measures, as well as transparent rules for legal protection in the executing State⁹.

In the era of technological advancement, effective cooperation in the administration of justice cannot exist without cross-border access to electronic evidence. Such cooperation was initiated by Directive 2014/41/EU

⁶ J. Sarkowicz, *The Role of the Principle of Mutual Recognition of Judicial Decisions in European Proceedings for the Gathering of Electronic Evidence: A Comparative Perspective*, "Prokuratura i Prawo" 2023, No. 12, p. 163.

⁷ In the original draft, no prohibition on issuing an Order on the basis of the *ne bis in idem* principle (Article 50 of the Charter of Fundamental Rights of the European Union and Article 54 of the Convention on Mutual Assistance in Criminal Matters) had been provided for, which required subsequent amendment. Consequently, Recital 46 incorporated the prohibition of double jeopardy. Nevertheless, the question arises as to how the issuing authority is supposed to become aware of such circumstances. No mandatory preliminary procedure for gathering information regarding these circumstances has been imposed on the issuing authority. If law enforcement authorities conducting an investigation are not sufficiently attentive to this issue, they may inadvertently overlook circumstances that could exclude the possibility of issuing an Order under Recital 46. According to this provision, the *ne bis in idem* principle constitutes one of the fundamental principles of EU law, recognized in the Charter of Fundamental Rights and developed in the case law of the Court of Justice of the European Union. Where the issuing authority has grounds to believe that parallel criminal proceedings may be pending in another Member State, it is required to consult the authorities of that Member State in accordance with Council Framework Decision 2009/948/JHA. In any event, a European Production Order or a European Preservation Order shall not be issued where the issuing authority has grounds to believe that doing so would be contrary to the *ne bis in idem* principle.

⁸ P. Topalnakos, *Critical Issues in the New EU Regulation...*, p. 202.

⁹ P. Topalnakos, *Critical Issues in the New EU Regulation...*, p. 203.

of 3 April 2014 on the European Investigation Order (Articles 589w et seq. of the Polish Code of Criminal Procedure)¹⁰. However, gathering electronic evidence through the European Investigation Order requires identification of the person using a specific telephone number or IP address. Furthermore, ordering the interception and recording of conversations requires cooperation and consent from the executing State. Therefore, one of the grounds for refusing recognition of an Order is the situation in which, under the law of the executing State, the investigative measure indicated in the EIO is restricted to a specified list or category of offences or to offences punishable by a certain maximum penalty, but does not include the offence indicated in the EIO¹¹.

The introduction of such a ground for refusal should be considered justified. If national law limits the use of one of these measures, such as wiretapping, to a specified category of offences or to offences punishable by a sufficiently severe penalty, there should be a possibility to refuse execution of the Order if it concerns an offence outside the catalogue provided for under national law. States should not be obliged to apply, for example, wiretapping solely because another Member State requests it, while such a measure would be inadmissible in a domestic case. This ground concerns investigative measures that interfere very deeply with civil rights¹².

Meanwhile, the new regulations concerning electronic evidence do not allow refusal in such situations. Moreover, European Production Orders

¹⁰ A European Investigation Order is a judicial decision issued or validated by a judicial authority of one Member State for the purpose of carrying out investigative measures in another Member State of the European Union in order to obtain evidence in criminal matters. The Directive on the European Investigation Order in criminal matters was adopted on 3 April 2014, and the deadline for transposition of the Directive into the national legal systems of the Member States expired on 22 May 2017. Denmark and Ireland are not bound by this instrument. The European Investigation Order is based on the principle of mutual recognition, which means that the executing authority is obliged to recognize a request issued by another Member State and ensure its execution. Execution is carried out in the same manner and under the same conditions as if the investigative measure had been ordered by an authority of the executing State. A European Investigation Order may also be issued for the purpose of obtaining evidence that already exists. The Directive provides a uniform and comprehensive framework enabling the gathering of evidence. Investigative measures include, for example, the hearing of witnesses, interception of telecommunications, covert investigations, and obtaining information concerning banking operations. Issuing authorities may make use of the European Investigation Order where its issuance is necessary, proportionate, and admissible in comparable domestic cases. See *European Investigation Order*, „e-Justice”, https://e-justice.europa.eu/content_evidence-92--maximize-pl.do [accessed: 1 July 2026].

¹¹ Article 11(1)(h): recognition or execution of a European Investigation Order in the executing State may be refused where, under the law of the executing State, the use of the investigative measure indicated in the EIO is limited to a specific list or category of offences, or to offences punishable by a certain maximum level of penalty, which do not include the offence specified in the EIO.

¹² G. Krysztofiuk, *The European Investigation Order*, “Prokuratura i Prawo” 2015, No. 12, p. 89.

and European Preservation Orders for electronic evidence significantly reduce the time required to obtain evidence compared to the European Investigation Order. Article 82 TFEU assumes cooperation between judicial authorities of the issuing State and the executing State. The new EU regulations on electronic evidence undermine this principle. In order to obtain evidence quickly, the judicial authorities of the executing State are bypassed. Instead, direct cooperation has been introduced between the competent authorities of the issuing State and private service providers¹³.

This allows the authorities of the issuing State to gain direct access to the data of citizens of another Member State without a decision by a court of the executing State and therefore without verification as to whether such access is lawful in a given case. Moreover, this access may concern sensitive personal data. At the same time, the only controller of the legality of interference with civil rights will be a private service provider, which cannot guarantee their effective protection¹⁴.

At the enforcement stage, the monitoring and information obligations imposed on the addressee (Articles 10(5)–(8) and 11(4)–(7) of the Regulation) are not capable of compensating for the shortcomings of the notification procedure towards the executing State. Addressees, namely private service providers, prove to be fundamentally unreliable defenders of fundamental rights. It is unclear on the basis of which criteria the addressee should conduct such review. Neither the addressee nor the service provider knows the significance of the data, nor do they always know the profession of the person whose data are concerned¹⁵.

Article 5(5) of the Regulation in conjunction with Article 9(2), first sentence¹⁶, provides that the information contained in the EPOC

¹³ J. Sarkowicz, *The Role of the Principle of Mutual Recognition...*, p. 169: “The authority recognizing and executing a European Production Order is the legal representative of the service provider, that is, a private entity. Such a situation is contrary to the principle of mutual recognition of judicial decisions”.

¹⁴ P. Topalnakos, *Critical Issues in the New EU Regulation...*, p. 201.

¹⁵ L. Krumwiede, *Das neue E-Evidence-Gesetzespaket – Eine kritische Analyse*, “*Zeitschrift für Internationale Strafrechtswissenschaft*” 2024, nr 3, p. 211.

¹⁶ The EPOC contains the information referred to in Article 5(5)(a)–(h), including sufficient information enabling the addressee to identify the issuing authority and the enforcing authority and, where necessary, to contact them.

(European Production Order Certificate) is limited to points (a)–(h)¹⁷. Additionally, service providers may be exposed to enforcement measures or sanctions in the event of non-compliance with the Order, which means they lack sufficient motivation to carry out a detailed review of the Order. This is particularly true because private service providers possess only limited resources for reviewing Orders¹⁸.

An additional threat is the short timeframe of the entire procedure for issuing the Order. This makes it almost impossible to verify its legality and justification. Moreover, severe financial penalties threatening service providers for breaches of the Regulation will discourage them from challenging the legality of Orders. Since contesting the legality of Orders would expose them to the risk of financial sanctions, it is obvious that they will be more inclined to ignore any irregularities connected with them rather than point them out¹⁹.

Failure to Inform the Executing State About a Preservation Order

The EU legislator attempted to prevent the above-mentioned threats. Article 8 imposes an obligation on the issuing authority to inform the enforcing authority in the executing State while simultaneously transmitting the so-called EPOC (European Production Order Certificate).

However, this notification obligation concerns only the issuance of a European Production Order and not the issuance of a European Preservation Order (EPOC-PR). Furthermore, it applies only to cases concerning traffic data or content data. A contrario, data used exclusively

¹⁷ Article 5(5): A European Production Order shall contain the following information: (a) the issuing authority and, where applicable, the validating authority; (b) the addressee of the European Production Order referred to in Article 7; (c) the user, except in the case of an Order whose sole purpose is the identification of the user, or any other unique identifiers, such as a username, login name, or account name, for the purpose of identifying the data covered by the Order; (d) the category of data covered by the Order according to the categories defined in Article 3(9)–(12); (e) where applicable, the time period for the data covered by the Production Order; (f) the applicable provisions of the criminal law of the issuing State; (g) in exceptional situations as defined in Article 3(18), duly justified reasons why the situation was considered exceptional; (h) where the European Production Order is addressed directly to a service provider that stores or otherwise processes data on behalf of a controller, confirmation that the conditions laid down in paragraph 6 of this Article are fulfilled.

¹⁸ L. Krumwiede, *Das neue E-Evidence-Gesetzespaket...*, p. 211.

¹⁹ L. Krumwiede, *Das neue E-Evidence-Gesetzespaket...*, p. 201.

for the identification of a user and subscriber will not require notification of the executing State²⁰.

During the legislative process, the Council of the European Union proposed that the enforcing authority should be notified in every case. Unfortunately, this proposal was not accepted by the Commission. Similarly, during trilogue negotiations, the European Parliament rightly proposed that, irrespective of the category of data, the executing authority should always be informed in every case involving either an EPO or an EPO-PR²¹.

While, for the purpose of effectively counteracting the risk of loss of electronic evidence, the absence of notification to the enforcing authority in the case of an EPOC-PR (European Preservation Order) may appear justified in order to achieve the legislator's objective of immediate preservation of data, once such preservation has been carried out, the risk of data loss ceases to exist. At that stage, there is sufficient time to provide notification. Therefore, an appropriate solution would be the introduction of a notification procedure for EPOs with regard to all categories of data²².

Deficiencies of the Notification Procedure Concerning the Production Order

As noted above, the notification obligation applies only to the issuance of a European Production Order and not to the issuance of a European Preservation Order (EPOC-PR).

However, the notification procedure has been regulated in a manner that raises significant doubts (see Article 8(1) of the Regulation).

²⁰ "Data requested solely for the purpose of identifying the user" means IP addresses and, where necessary, the relevant source ports and time stamps, namely the date and time or the technical equivalent of those identifiers and related information, where such data have been requested by law enforcement or judicial authorities solely for the purpose of identifying the user in a specific criminal proceeding (Article 3(10) (Definitions) of the Regulation).

²¹ In German legal scholarship, the adopted solution has been criticized as infringing sovereignty and civil liberties: see L. Krumwiede, *Das neue E-Evidence-Gesetzespaket...*, p. 210.

²² L. Krumwiede, *Das neue E-Evidence-Gesetzespaket...*, p. 210.

Namely, the enforcing authority²³ does not need to be notified by the issuing authority if the person whose data are covered by the Order resides in the issuing State (Article 8(2)(b)). Since the criterion of residence in the issuing State constitutes a substantial derogation from the principle of notification, it should be defined precisely, which unfortunately is not the case.

According to Recital 53, the assessment by the issuing authority²⁴ should be based on objective circumstances. In this context, the characteristic of “residing in the issuing State” constitutes an appropriate indicator for assessing a person’s place of residence. However, circumstances intended to indicate residence, rather than mere “presence,” appear problematic, such as the intention to “settle in that Member State” or the existence of “certain ties” with a given State, for example “family or economic ties.” At the same time, a short holiday or vacation stay without additional connections would not be sufficient (see Recital 53). There are many situations in which the lack of sufficient precision in determining these criteria makes it possible to argue almost arbitrarily both for and against recognizing a person as residing in a given State.

Moreover, the procedure for verification of the Order by the enforcing authority has not been precisely developed. Only Article 12(1) of the Regulation imposes on it the obligation to assess the information contained in the Order and indicates the grounds for refusal. Consequently, doubts arise as to whether the Order will in fact be properly reviewed by the executing State within the prescribed timeframe. These concerns are further reinforced by the fact that as many as nine Member States expressed reservations regarding the notification procedure. Among them was Ireland, where major American companies such as Google, Meta Platforms, and X (Twitter) are headquartered²⁵.

The wording of Article 12(1)(b) of the Regulation, which sets out the grounds for refusing execution of European Production Orders, is rather restrictive. Such refusal is limited to “exceptional situations”

²³ “Enforcing authority” means an authority in the executing State which, in accordance with the national law of that State, is competent to receive a European Production Order and EPOC or a European Preservation Order and EPOC-PR transmitted by the issuing authority, for the purpose of notification of the Order or for the purpose of enforcing the Order in accordance with this Regulation: Article 3(17) of the Regulation.

²⁴ “Issuing authority” means the competent authority in the issuing State which is empowered, in accordance with Article 4, to issue a European Production Order or a European Preservation Order: Article 3(15) of the Regulation.

²⁵ L. Krumwiede, *Das neue E-Evidence-Gesetzespaket...*, p. 211.

where “there are substantial grounds to believe, on the basis of specific and objective evidence, that execution of the Order in the particular circumstances of the case would entail a manifest breach of a relevant fundamental right set out in Article 6 TEU and the Charter.” This may result in the executing State being exceptionally reluctant to refuse execution of Orders.

Likewise, the principle of double criminality referred to in Article 12(1)(d) is significantly limited. The acts listed in Annex IV are excluded from its application²⁶. In the absence of a requirement of criminality in the executing State, there is a risk that politically motivated Orders may be enforced²⁷.

It should also be emphasized that personal data, including identifying data such as IP addresses, require special protection both at the European level (under Article 6(1) TEU in conjunction with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union) and at the national level.

As can be seen, the Regulation fundamentally altered the principles of EU primary law. Traditionally, those principles were limited to facilitating judicial cooperation between States. By contrast, this legal act introduced cooperation between States and private entities. Consequently, key elements traditionally present in EU regulations, such as mutual recognition, are missing²⁸.

Violation of Sovereignty

The principle of territorial sovereignty primarily serves to preserve and ensure standards of protection of fundamental rights and personal data. A State is obliged to respect and protect the fundamental rights

²⁶ These offences are characterized by a significant degree of generality, as it is difficult to determine how precisely the constituent elements of offences such as “xenophobia” or even “computer crime” are to be defined.

²⁷ L. Krumwiede, *Das neue E-Evidence-Gesetzespaket...*, p. 211.

²⁸ S. Buczman, *Mutual Recognition of Criminal Judgments in the European Union. A Practitioner's Guide*, R. Kierzyńska (ed.), Kraków 2023, p. 120: “Whereas the classical mechanism of international mutual legal assistance is based on a request from the requesting State, the execution of which is largely subject to the discretionary assessment of the requested State, cooperation based on mutual recognition relies on a far-reaching automatism of recognition of the decision by the executing State. That State may refuse cooperation only on the basis of strictly defined negative grounds, largely of a formal nature, for the execution of the decision.”

and personal data of persons located within its territory not only when exercising its own public authority, but especially within the framework of international cooperation in criminal matters²⁹.

A minimum level of protection of fundamental rights must be ensured where the participation of the executing State is entirely absent. This absence should be compensated for by strict requirements imposed on the issuing State when issuing Orders. Unfortunately, this is not the case. These gaps in the notification mechanism are not compensated for by stringent requirements concerning the issuing decision³⁰.

First, the Regulation does not provide for an appropriate hierarchy between the Production Order and the Preservation Order. This alone is problematic. Consequently, issuing authorities have discretionary freedom to choose, in certain cases, a Production Order instead of a Preservation Order. The interference with personal data is then more intensive (in the case of an EPO than in the case of an EPO-PR), while the required conditions are less stringent. Yet State interference with personal rights should be limited to the absolute minimum necessary.

Additionally, Article 5(5)(e) of the Regulation, which provides that “where necessary” the time limit for the production of data should be specified, does not ensure sufficient precision regarding the scope of such interference. With regard to EPOs concerning subscriber and identification data, no clear grounds for their issuance have been introduced, nor has exclusive competence of courts been guaranteed (Article 4 of the Regulation), despite the fact that such measures constitute significant interference with the right to privacy, thereby further undermining the effectiveness of fundamental rights protection. In essence, this amounts to surveillance without a court decision.

Second, the EU legislator failed to provide sufficient protection for immunities and for freedom of the press and freedom of expression. Although Article 5(10) of the Regulation establishes a review mechanism concerning the protection of these values, it is limited solely to EPOs involving traffic and content data. Such protection was excluded in the case of EPOs concerning subscriber and identification data. Yet such data may also reveal important information regarding a user’s behaviour, habits, and routines. Therefore, an obligation should be introduced requiring

²⁹ M. Böse, *Der Kommissionsvorschlag zum transnationalen Zugriff auf elektronische Beweismittel – Rückzug des Staates aus der Rechtshilfe?*, „Kriminalpolitische Zeitschrift” 2019, nr 3, pp. 140–143.

³⁰ M. Böse, *Der Kommissionsvorschlag zum transnationalen Zugriff...*, p. 143.

the issuing authority to conduct a review, irrespective of the category of data, with regard to possible immunities and special civil guarantees, as well as freedom of the press and freedom of expression.

The above solution creates the danger that the instruments provided for in the Regulation may be misused to identify, for example, political opponents, journalists and their sources, or whistleblowers³¹.

Third, with regard to Article 5(10) of the Regulation³², the question arises as to how the issuing authority is supposed to obtain knowledge concerning possible immunities, privileges, or guarantees of freedom of the press and expression under the law of the executing State. No obligation to verify the existence of such circumstances has been established. Such verification should already occur at the preliminary stage preceding the issuance of the Order. Furthermore, Article 5(10) of the Regulation does not refer to States in which the persons covered by the Order reside or from which they may derive their immunities. Yet it is precisely those States that, in the name of protecting their sovereignty, should have the right to reserve protection for their own citizens.

To summarize the above, the absence of notification to the executing State regarding the Order creates a serious risk of violating its sovereignty and the fundamental rights of its citizens.

Hence, the criticism rightly expressed in German legal scholarship that the notification mechanism contains serious loopholes and that compensatory decision-making bodies capable of offsetting these deficiencies have not been established, at the expense of the protection of fundamental rights³³.

³¹ L. Krumwiede, *Das neue E-Evidence-Gesetzespaket...*, p. 211.

³² Where the issuing authority has reason to believe that traffic data—except for data requested solely for the purpose of identifying the user as defined in Article 3(10)—or content data covered by a European Production Order are protected by immunities or privileges under the law of the executing State, or that such data are subject in that State to rules on the determination and limits of criminal liability related to freedom of the press or freedom of expression in other media, the issuing authority may seek clarifications prior to issuing the European Production Order, including through consultations with the competent authorities of the executing State, either directly or via Eurojust or the European Judicial Network.

³³ L. Krumwiede, *Das neue E-Evidence-Gesetzespaket...*, p. 210.

Abandonment of the Principle of Double Criminality and the Principle of Speciality

The principle of double criminality is increasingly regarded as a principle of customary international law. It constitutes one of the structures embedded in criminal proceedings containing a transnational element. In criminal proceedings involving international relations, it is perceived as a prerogative of the State, which thereby retains the right to limit cooperation in international legal relations only to conduct that it itself subjects to criminal repression³⁴.

Its abandonment cannot be justified by the potential gain of more efficient and faster cooperation between States. A service provider in the executing State will be obliged to undertake actions aimed at punishing a person for conduct that is entirely lawful within that State. At the same time, the authorities of that State will impose coercive measures on their own citizens for conduct that is not unlawful under domestic law. If the act had been committed within its territory, those authorities would not possess such powers.

Admittedly, Article 12(1)(d) in conjunction with Article 8 of the Regulation provides that lack of double criminality constitutes a ground for refusing a European Production Order. However, this does not apply to a specified category of offences punishable by up to three years' imprisonment. Furthermore, the principle of double criminality applies only where the request concerns two categories of data simultaneously: traffic data and content data. It does not apply where the request concerns solely subscriber and user data. In such a case, obtaining those data is possible even if the surveilled person staying within the territory of the executing State has not committed an offence under the legislation of that country.

Moreover, the principle of double criminality does not apply at all to European Preservation Orders, regardless of whether they concern only user or subscriber identification data, traffic data, or content data.

The Regulation remains entirely silent on the principle of speciality. The Directive on the European Investigation Order had already departed

³⁴ L. Brodowski, *The Principle of Double Criminality in the Context of Extradition*, „Studia Prawnicze KUL” 2015, nr 1, p. 31.

from this principle. Consequently, electronic evidence obtained for a specific case may be used for entirely different purposes than the particular proceedings in which it was acquired.

Safeguards for individuals against the Orders discussed here are available to suspects, accused persons, and third parties, but exclusively in relation to European Production Orders. They may challenge the legality, necessity, and proportionality of those measures before the competent authorities of the issuing State. At the same time, European Preservation Orders are deprived of any civil guarantees. The legislator assumed that such an Order does not itself result in disclosure of data. Only when a European Production Order is subsequently issued may it be reviewed pursuant to Article 18 of the Regulation.

Irrespective of the above, the service provider is, under national law, obliged to delete data intended for preservation in accordance with a European Preservation Order.

The retention of data pursuant to a European Preservation Order, where such data should otherwise be deleted, results in a violation of the right to privacy and protection of family life. Furthermore, the retention period for data held by the service provider may be extended from the initial 60 days by an additional 30 days (Article 11(1) of the Regulation), and subsequently for an indefinite period until a European Production Order is either issued or withdrawn.

The Regulation lacks provisions guaranteeing the availability of legal remedies in the executing State³⁵. Persons affected by such Orders will therefore be forced to resort to remedies in the issuing State. This, however, will be highly burdensome. Their only consolation is the general principle expressed in Article 18(2) in fine of the Regulation, according to which the right to an effective remedy is exercised before a court

³⁵ For the effective exercise of the right to appeal, information about the decision being challenged is necessary. However, although Article 13(1) of the Regulation provides for notification of the Order, Article 13(2) introduces a problematic exception. Under this provision, the issuing authority may, in accordance with the national law of the issuing State, delay or restrict notification to the person whose data are covered by the Order, or refrain from notifying them altogether, insofar as the conditions laid down in Article 13(3) of Directive (EU) 2016/680 are fulfilled, and for as long as those conditions continue to be met. In such cases, the authority must state in the case file the reasons for the delay, restriction, or non-notification. This may lead to situations in which the person affected by the measure is unable to challenge the Order or is not even aware of its existence. This is particularly likely where, in the course of an investigation, data are transmitted under a European Production Order but ultimately no charges are brought. The situation is especially problematic where the executing State has not been involved at all in the process. Unfortunately, the proposal of the European Parliament that the decision to apply such an exception should be subject to judicial authorization was not accepted.

in the issuing State in accordance with its national law and includes the possibility of challenging the legality of the measure, including its necessity and proportionality, without prejudice to fundamental rights guarantees in the executing State. In the absence of other regulations in the executing State, this provision should be interpreted as a regulatory norm permitting verification of the legality and justification of the Order by the executing State upon request of a person subject to its jurisdiction, rather than merely as a general guiding principle.

Furthermore, the Regulation does not provide for exclusionary rules concerning evidence obtained unlawfully. Without such exclusionary rules, as emphasized by the European Parliament, the limitations contained in the Regulation will not ensure sufficient protection of fundamental rights³⁶. In particular, there is no effective protection of fundamental rights with regard to persons who, under national law, possess the right to refuse to testify, nor with regard to categories of persons whose data require special protection under national law³⁷.

The General Data Protection Regulation (GDPR), in Article 5(1)(d), provides that personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (“accuracy”). This provision expresses the principle that the purpose of processing personal data determines their legality and accuracy.

The Council and the European Parliament proposed that the Regulation discussed here should contain similar provisions defining the further use of personal data or limiting their use exclusively to their original purpose. Unfortunately, these proposals were not accepted by the European Commission.

³⁶ The absence of exclusionary rules on the use of evidence in judicial proceedings with respect to data obtained unlawfully is contrary to the data protection principle established under European data protection law (see L. Krumwiede, *Das neue E-Evidence-Gesetzespaket...*, p. 212). This principle is enshrined in Article 5(1)(a) of the GDPR, which requires that personal data be processed lawfully, fairly, and in a transparent manner in relation to the data subject (“lawfulness, fairness and transparency”). It is further reflected in Article 17(1)(d) GDPR, which provides that the data subject has the right to obtain from the controller the erasure of personal data concerning them without undue delay, and the controller is obliged to erase personal data without undue delay where the data have been processed unlawfully. In addition, it is reflected in Article 4(1)(a) of Directive (EU) 2016/680, which requires Member States to ensure that personal data are processed lawfully and fairly.

³⁷ L. Krumwiede, *Das neue E-Evidence-Gesetzespaket...*, p. 212.

Conclusion

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 raises substantial concerns.

First and foremost, it infringes the principle of sovereignty³⁸ and the related principle of mutual recognition of judicial decisions (Article 82 TEU), which in turn constitutes a guarantee of compliance with numerous rights of suspects and accused persons³⁹. This leads to violations of fundamental rights.

Furthermore, the Regulation abolishes the requirement of double criminality. This will result in the collection of data concerning acts that are not regarded as criminal offences in the executing State. Additionally, the absence of the principle of speciality creates the risk of arbitrary and discretionary use of the evidence obtained.

Unfortunately, the Regulation does not provide clear legal protection mechanisms for persons subjected to surveillance⁴⁰.

³⁸ M. M. Böse aptly summarized this issue, stating that the protection of territorial sovereignty lies not only in the interest of Member States, but also—and above all—in the interest of protecting the fundamental rights of their citizens: M. Böse, *The Commission Proposal on Transnational Access...*, p. 143. Territorial sovereignty is inseparably linked to the State's obligation to respect and protect the fundamental rights of persons within its territory in the exercise of its public authority. This also applies to cross-border cooperation in criminal matters, within which minimum standards of human rights and the rule of law must be ensured. These requirements must likewise be taken into account in the context of cross-border data transfers. However, as a result of the "automatic" recognition of orders, the executing State is no longer able to fulfil its responsibility for the protection of fundamental rights. These risks were highlighted both by the Bundesrat and by the European Parliament.

³⁹ Cf. M. Böse, *An Assessment of the Commission's Proposals on Electronic Evidence*, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies of the Union, European Parliament (PE), September 2018.

⁴⁰ M. Böse, *Der Kommissionsvorschlag zum transnationalen Zugriff...*, p. 146.

Bibliography

- Brodowski L., *The Principle of Double Criminality in the Context of Extradition*, „Studia Prawnicze KUL” 2015, nr 1
- Buczma S., *Mutual Recognition of Criminal Judgments in the European Union. A Practitioner's Guide*, R. Kierzyńska (red.), M. Stefaniak-Dąbrowska, Kraków 2023
- Böse M., *An Assessment of the Commission's Proposals on Electronic Evidence*, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate-General for Internal Policies of the Union, European Parliament (PE), September 2018
- Böse M., *Der Kommissionsvorschlag zum transnationalen Zugriff auf elektronische Beweismittel – Rückzug des Staates aus der Rechtshilfe?*, „Kriminalpolitische Zeitschrift” 2019, nr 3
- E-evidence – cross-border access to electronic evidence*, „Consilium”, <https://www.consilium.europa.eu/pl/policies/e-evidence/>
- E-evidence – cross-border access to electronic evidence*, „European Commission”, https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en
- European Investigation Order*, „e-Justice”, https://e-justice.europa.eu/content_evidence-92--maximize-pl.do
- Krumwiede L., *Das neue E-Evidence-Gesetzespaket – Eine kritische Analyse*, „Zeitschrift für Internationale Strafrechtswissenschaft” 2024, nr 3
- Krysztofiuk G., *The European Investigation Order*, „Prokuratura i Prawo” 2015, nr 12
- Sarkowicz J., *The Role of the Principle of Mutual Recognition of Judicial Decisions in European Proceedings for the Gathering of Electronic Evidence: A Comparative Perspective*, „Prokuratura i Prawo” 2023, nr 12
- Topalnakos P., *Critical Issues in the New EU Regulation on Electronic Evidence in Criminal Proceedings*, „eucrim” 2023, nr 2