Raimundas Jurka

The E-Evidence "Movement" in European Union Criminal Justice: Toward or Beyond Coherence?

The free "movement" of evidence without being hindered in the context of the criminal justice system of the European Union (hereinafter referred to as the "EU") and its Member States is a real challenge for both EU legislation and the platform for judicial cooperation between the Member States. The legal proceedings of collecting and transferring evidence, in particular electronic evidence, from one Member State to another not only depend on consistency within these proceedings and the interconnectivity of these processes based on cooperation established between Member States, but should be also admissible as evidence in the national court of any given Member State in criminal proceedings concerning a particular person. Thus, perceiving the whole process as an integral cross-compliance mechanism, the coherence and proportionality of EU legal instruments may also be subject to evaluation between courts of Member States in the field of collecting electronic evidence during criminal proceedings.

The optimization of legislative procedures in all matters related to gathering evidence across EU Member States for the EU criminal justice system provides an opportunity to see how attitudes toward the process of gathering electronic evidence are changing. Although this process continues to be based on the maxim of mutual recognition, which, at least theoretically, ensures the confidence of Member States in each other's legal systems and judicial decisions, the development of the legal instrumentation in question also reveals certain threats to legal assessment, the fragmentation of the regulatory framework, and the not entirely justified and reasonable differentiation of the collection of evidence depending on the type of evidence being collected.

It is therefore crucially important to understand not only what drives the changes and developments in EU legislation on electronic evidence, but also the need to maintain this legal framework as a harmonious and coherent process. However, there is nothing wrong or harmful with the notion that the modernization of social relationships also implies the need to modernize the arrangements for judicial cooperation based on the principle of mutual recognition. On the other hand, another equally important issue cannot be ignored: the recognition of electronic evidence and its admissibility in particular criminal proceedings.

This is the actual aim of the free movement of evidence among Member States in EU criminal justice.

The abovementioned insights allow for the identification of the following scientific problems that are analyzed in this research: what are the factors that cause EU legal regulation in the sphere of the evidence making procedure in criminal justice to become fragmented? Does the EU legal regulation in the sphere of e-evidence collection create preconditions to ensure the principles of the right to a fair trial in criminal justice?

Cross-Border Access to Electronic Evidence Within the European Union: Reasons and Regulatory Background

As of April 2018, when the first version of the European Commission's proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters appeared, after protracted discussions and lengthy negotiations, Regulation (EU) 2023/1543 of the European Parliament and of the Council on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and the execution of custodial sentences following criminal proceedings (hereinafter referred to as the "Regulation") was adopted on 12 July 2023. This is likely the first document of its kind that modifies the traditional model of mutual recognition and mutual legal assistance agreements (Corhay 2023b). It signals a shift from the traditional model of judicial cooperation based on mutual recognition toward substantially "operational" (European Digital Rights 2023) cooperation between the competent law enforcement authorities of a Member State and a service provider (as defined in Article 3(3) of the Regulation). The latter initiative has indeed caused considerable controversy, generating both positive and critical evaluations, as reflected in various sources. According to one source (Corhay 2023a), it institutionalizes the criminal justice paradigm – i.e., immediate and direct cooperation between law enforcement, judicial authorities and the private sector (service providers). Corhay (2023a) points out that "unlike other forms of cooperation in criminal matters regulated by EU law which involve the cooperation between judicial authorities of different Member States – like the European Arrest Warrant and the European Investigation Order – the original e-evidence proposal substitutes the traditional executing Member States by a private actor," and even expresses her concern that this new model allows the involvement of the law enforcement or judicial authorities of the executing State to be bypassed in the cooperation process. Some sources even use sarcasm, observing that such a model presupposes

turning private sector companies providing electronic communications services into "private law enforcement agencies" (Petri 2018). According to Petri (2018), "criminal investigation and law enforcement are sovereign tasks. They must generally remain in the hands of government bodies in the respective country and must not be delegated to private enterprises. Likewise, the home country of the provider who is obliged to cooperate, needs to be enabled to ensure the legitimacy of the order according to its national law. This is the only way to ensure compliance with legal rules governing criminal prosecution." At the same time, there is no denying that "it should be stressed that the proposed Regulation is much more comprehensive and detailed compared to the previous legal documents in that area. The proposal targets directly the specific problem created by the volatile nature of the electronic evidence and its international dimension" (Blažič and Klobučar 2020, p.98).

These and other assessments thus show that the Regulation, which introduces a rather revolutionary model of judicial cooperation that directly involves private sector entities, is indeed met with a certain amount of mistrust. Paradoxically, the Regulation implements the principle of mutual recognition; at the same time, however, the doctrine expresses doubts as to whether the mechanism set out in the Regulation will ensure the recognition of electronic evidence as a standard of achievement to be pursued.

Indeed, as will become apparent below, the new regulatory framework on so-called cross-border access to electronic evidence is controversial, as it is interpreted and understood in different ways. It is certainly true that it would be objectively impossible to disclose all assessments in this paper due to its limited scope, but one aspect of the subject will certainly be touched upon. The question will be whether this regulation will indeed allow for the admissibility of transmitted electronic evidence and the coherence of this process in the EU criminal justice system.

When putting the emphasis on the substance of the Regulation adopted by the Council on cross-border access to electronic evidence as an innovation in the EU for the optimization of judicial cooperation in the field of criminal justice, the reasons that have led to this innovation should be identified.

Firstly, the means of receiving and storing electronic evidence are becoming increasingly important for criminal proceedings throughout the EU. Effective mechanisms for collecting electronic evidence are essential in combating crime and should be subject to conditions and safeguards that ensure full compliance with the fundamental rights and principles recognized by Article 6 of the Treaty on European Union and the Charter of Fundamental Rights of the European Union, in particular the principles of necessity and proportionality,

due process, privacy and the protection of personal data, and the confidentiality of communications.

Secondly, services based on electronic communications networks can be provided from any location and do not require physical infrastructure, premises or staff in the country where the service is being offered. As a result, electronic evidence is often stored outside the borders of the investigating State or is stored by a service provider located outside the territory of that State, posing challenges for the collection of electronic evidence and obtaining proof in criminal proceedings. That implies, amongst other things, that the "globalization of criminal evidence" (Swire and Kennedy-Mayo 2017, cited in Abraha 2020, p.327) makes the territorial scope of the protection of criminal jurisdiction less relevant. Furthermore, according to Tosza (2020, pp.168–169), "investigative authorities depend much more significantly on the cooperation of service providers also for practical reasons. While a raid on a company that refuses to produce requested documents would be a viable possibility, a raid on a data center would not bring similar (if any) results, unless disproportionally significant forces are used to find the necessary data, potentially including heavy decrypting capacities if that was possible at all". This idea is echoed by Rojszczak (2022), who claims that

> the global nature of many digital services means that identifying the obliged entity may not be a straightforward task. In many cases, the service provider may have several (multiple) representative offices within the EU. On the one hand, leaving the authorities of the requesting state free to choose which office to address their request for data access to meets the objective of efficient criminal proceedings, but, on the other hand, it makes it difficult to control the decisions taken. In particular, a court order that does not allow the transfer of electronic evidence in one Member State may not prohibit the authorities of the requesting State from making an identical request to another Member State (p.1002).

Thirdly, the procedures and time limits set out in Directive 2014/41/EU of the European Parliament and of the Council of April 3, 2014 regarding the European Investigation Order in Criminal Matters (hereinafter referred to as "EIO Directive" or "EIO"), and in the Convention on mutual assistance in criminal matters between the EU Member States approved by the Council under Article 34 of the Treaty on the European Union (hereinafter referred to as the "Convention"), are not appropriate for electronic evidence, which is more volatile and can be easily and rather quickly deleted. Obtaining electronic evidence through channels for data and judicial cooperation requests is often time-consuming and may result in information being unavailable in the future. Moreover, as is pointed out in the Explanatory Memorandum to the Proposal for a regulation of electronic evidence in criminal matters, the EIO Directive, which

has profoundly changed the Convention, applies to any investigative measure and includes access to electronic evidence, but the EIO Directive does not contain any specific provisions relating to this type of evidence. It is highlighted that the Regulation will not replace the EIO, which is aimed at obtaining electronic evidence, but that the Regulation provides an additional instrument available to national authorities. There may also be situations where, for example, several investigative measures need to be applied in the executing Member State and the authorities may prefer the EIO. The creation of a new instrument concerning electronic evidence is a better alternative than amending the EIO Directive when dealing with the specific challenges and problems of collecting electronic evidence, which do not affect the other investigative measures provided for in the EIO Directive (European Commission 2018). Moreover, there is no harmonized framework for cooperation with service providers, although some third-country service providers accept direct requests for such data as authorized according to their own State's national law. However, the practice employed by law enforcement authorities indicates that in reality, a number of requests to service providers/their representatives located in another EU Member State to provide the relevant electronic data remain unfulfilled because service providers are simply not obliged to comply with such requests, which has a particular impact on the work of law enforcement and the implementation of the procedural guarantees of the participants involved in criminal proceedings (Tosza 2020, p.169). Moreover, as Tosza notes, "the increasing need to obtain data for criminal investigation combined with these difficulties and the volatility of data creates the need to find a solution which would facilitate this process. The EIO may serve to acquire electronic evidence, but it is claimed that for that its deadlines are too long and create a risk that data disappears or is altered in the meantime. Nor can it resolve the question of territoriality" (p.169).

It would indeed be possible to identify more reasons for the regulation of the collection of electronic evidence in criminal proceedings. However, it has become apparent that the purpose of the new regulation is unquestionable, and it is therefore not very reasonable to limit ourselves solely to this aspect any further. What is even more important is whether the chosen regulatory model will be able to ensure the implementation of the objective of the "movement" of electronic evidence in the EU criminal justice system. In other words, whether this evidence, once it has been collected following the procedure laid down in the Regulation, will be admissible as evidence in the national court of the issuing Member State in the context of the European Production Order (hereinafter referred to as the "EPO"). Before proceeding to the analysis of this issue, it is therefore necessary to briefly summarize the substance of this Regulation.

The Regulation aims to establish a mechanism as an alternative to preexisting instruments of international cooperation and mutual legal assistance in criminal matters. In particular, it seeks to address the problems arising from the volatile nature of electronic evidence and the "non-locality" aspect by creating new procedures for rapid, efficient and effective cross-border access. The Regulation establishes the system for European Evidence Production and Preservation Orders, which can be issued by judicial authorities to obtain or preserve electronic evidence, regardless of the location of the data. These orders can be issued to any category of data, including subscriber data, traffic (flow) data, content data, etc. The Regulation governs only the collection of data stored by the service provider at the time of obtaining an EPO or a European Preservation Order, prior to a specific criminal proceeding relating to a specific criminal offense that has already been committed, based on a case-by-case assessment of the necessity and proportionality of the orders and taking into account the rights of the suspect or accused person.

The mechanism for the use of the EPO and European Preservation Order in criminal proceedings for electronic evidence is thus based on the principle of mutual trust between Member States and, at the same time, on the presumption that Member States are compliant with EU legislation, follow the rule of law and comply with fundamental rights, which are essential elements of freedom, security, and justice within EU. On the contrary, without taking into account the relationship between the powers of the state and mechanisms of protection of fundamental rights, the problem of developing a coherent model of cross-border cooperation in the transmission of electronic evidence cannot be solved (Rojszczak 2020, p.13). This mechanism allows the law enforcement and judicial authorities of Member States to issue orders directly to service providers. One point which is very important in this regard is the fact that the assessed legal mechanism must also be based on the implementation of procedural rights in criminal proceedings as laid down in Directives 2010/64/EU1, 2012/13/EU2, 2013/48/EU3, (EU) 2016/3434, (EU) 2016/8005, and (EU) 2016/19196 of the European Parliament and of the Council. In addition, it must be observed that these orders can only be issued in the light of the rights of the suspected or accused person in proceedings relating to a criminal offense, and only if such an order could be issued under the same conditions in a similar domestic case, and, consequently, if the suspected or accused person is entitled to an effective remedy in the course of criminal proceedings in which the collected data are used as evidence (the right to an effective remedy should be exercised before the court of the issuing State following its national law, and should include the possibility to challenge the legality of the measure, including its necessity and

proportionality). In this respect, it should be noted that, in the context of the relationship governed by the Regulation, it is particularly important to safeguard the procedural interests not only of suspects and accused persons in the Member State of the issuing authority, but also in the State of the executing authority (Kosta and Kamara 2023, p.74). In assessing whether orders may be issued, it is necessary to consider whether the order is limited to what is necessary to fulfil a legitimate objective, i.e., to obtain data that is relevant and necessary evidence in a particular case.

To sum up very briefly, it can be considered that the new regulation on the collection of electronic evidence in criminal proceedings, which contributes to the coordination, sustainability, legal clarity, transparency, and accountability of the EU criminal justice system (Warken, van Zwieten and Svantesson 2020, p.49), is a continuation of the development of mutual recognition among Member States in EU criminal justice. The Regulation under examination establishes a new type of judicial cooperation model by avoiding the involvement of the judicial or law enforcement authorities of the executing authority in the recognition and execution of orders. Instead, it establishes a space for the issuing state to approach service providers normally belonging to the private sector directly (following the principle of direct communication (Jurka 2019, p. 322)), thus moving from a horizontal to a vertical cooperation model. At the same time, it should be noted that the aforesaid regulation which is being examined does not replace other EU legislation in matters related to gathering evidence. On the contrary, the new regulation creates a kind of differentiation in the collection of evidence in criminal proceedings.

The Relationship Between the European Investigation Order and the Regulation on Electronic Evidence

It should be recalled that the purpose and essence of the EIO Directive, unlike previous EU legislation that intends to facilitate judicial cooperation in the taking of evidence in criminal proceedings, is not only to collect, record, and transmit evidence already existing in other EU Member States, but also to carry out the actions of searching for, collecting, receiving, and transmitting evidence to the issuing State. In other words, the EIO mechanism is based on a twofold system of evidence gathering: on the one hand, it may collect and transmit existing evidence (retrospective data); at the same time, it may be used for searching, capturing, and collecting evidence of interest to a Member State's law enforcement authority in real time (prospective data). The scope of the EIO thus extends beyond the process of gathering evidence to include procedural steps (measures)

to search for and collect such evidence – in particular, evidence that has not yet been gathered. The purpose of the EIO Directive is not only to collect pre-existing evidence but also to request that another EU Member State take legal proceedings to collect relevant evidence of interest to the issuing Member State (Jurka 2011, p.116). For instance, Article 5(1)(e) of the EIO Directive states that "the EIO shall, in particular, contain the following information: […] a description of the investigative measures(s) requested and the evidence to be obtained." This is in line with the principle that "the executing authority shall comply with the formalities and procedures expressly indicated by the issuing authority unless otherwise provided in this Directive and provided that such formalities and procedures are not contrary to the fundamental principles of the law of the executing State." The executing competent authority may also have recourse to an investigative measure(s) other than that indicated in the EIO, where the investigative measure(s) selected by the executing competent authority would achieve the same result by less intrusive means than the investigative measure(s) indicated in the EIO. Thus, the Member State that requests another Member State to search for and collect the necessary evidence specifies the investigative steps that should be taken to ensure that the subsequent collection and receipt of such evidence does not create additional problems in ensuring the admissibility of such evidence, as the procedural requirements for the collection of evidence (and the procedural form for the collection of the data) may be different in the requesting State and the executing State (Belevičius 2013, p.183). This implements the requirement of *forum regit actum*, according to which a request for judicial cooperation is implemented following the national law of the requesting State.

The model of judicial cooperation created by the EIO Directive and applied in a truly effective manner does not differentiate the evidence to which the Directive applies; it does not matter whether it is personal or material evidence, whether it is tangible or digital data. In addition to these innovations (in terms of the *forum regit actum* option, which allows EU Member States not to unify the principles of data collection in their laws on criminal procedure, which, due to different legal and social traditions, could not be unified (Mangiaracina 2014, p.116); there are also opponents of this system who argue that *forum regit actum* as a consequence of the principle of mutual recognition does not resolve the issue of admissibility of evidence: "the EU, when developing the EIO Directive, did not take advantage of Article 82(2) TFEU which allows for the introduction of common EU minimum standards facilitating the admissibility of evidence. Instead of this, the EIO still relies on the *forum regit actum* principle, which has questionable potential to ensure mutual recognition of evidence in the" (Kusak

2019, p.399)), the traditional procedure for the implementation of the principle of mutual recognition has also been preserved, involving aspects such as the legal status of the issuing authority and the executing authority, the communication of these competent authorities, the procedures for the issuance, transmission, recognition, and execution of the EIO, the grounds for non-recognition and non-enforcement, the grounds and conditions for the application of alternative investigative measures, etc. Indeed, for the sake of accuracy and completeness, it should be noted that although the provisions of the EIO Directive are general in nature (it should be noted that when the proposal (draft) of this Directive was still being considered, it was strongly believed that the provisions of this legal instrument would fully cover the collection of electronic evidence (Leroux 2004, pp.193–220)) and are intended for and applicable to almost all types of evidence, Article 10(2)(e) and Article 30 of this Directive specifically provide for what investigative instruments and measures are intended for the collection of electronic evidence, i.e., the identification of persons holding a subscription of a specified phone number or IP address and the interception of telecommunications with the technical assistance of another Member State.

Regarding the relationship between the EIO and the Regulation, Corhay (2023a), analyzing the cooperation model established by the Regulation on electronic evidence in criminal proceedings and comparing it with the principle of the application of the EIO Directive, notes that "the e-evidence proposal is fundamentally different from the European Investigation Order (EIO) which require the order to be circulated between and executed by competent authorities (for a comparison between the two instruments). The competent authority receiving the order performs the necessary checks and assesses it against several grounds for refusal. While the EIO was meant to offer a comprehensive solution to cross-border gathering of evidence, it was not tailored specifically for the collection of electronic evidence which resulted in some significant shortcomings."

Thus, in the doctrinal sources, one can find a variety of assessments that reveal the relationship between the discussed evidence-collection mechanisms, including their similarities and differences. This relationship provides a basis for understanding the peculiarities of the analyzed mechanisms and the fundamental differences that led to the EU legislative decision not to combine the two mechanisms into a single one – for example, into one governed by the EIO Directive.

The two regulatory mechanisms in question, the Regulation and the EIO Directive, are essentially similar in many respects: the identical or at least very similar (Tosza 2020, p.177) objectives; the common legal basis provided for in Article 82(1) of the Treaty on the Functioning of the European Union (2012);

the traditional (customary) system of issuing orders (the requirement to issue an order following the principles of necessity and proportionality, the criterion of similar domestic cases, etc.), and so on. However, there are also substantial, even fundamental differences that allow us to answer why it was decided to regulate the relationship governed by the Regulation (the process of collecting electronic evidence) by enacting a separate piece of legislation rather than integrating these provisions into the time-tested mechanism of the EIO Directive.

The first and most fundamental difference can be found in the prerequisites for issuing an order. Whereas the EIO is based on the free movement of persons and the abolition of borders, the EPO is based on so-called cyberspace, which has no physical borders. This therefore means that the free movement of persons is not necessary for the issuing of an EPO: "There may be need for an EPO in a purely domestic case, with perpetrators, victims, place of commission and investigating authorities all from one locality, just because the data that are needed happen to be in possession of a service provider from another member state" (Tosza 2020, p.177). It is sufficient, therefore, that the data required in the criminal proceedings are managed by a service provider established or otherwise operating in another Member State.

Secondly, the Regulation establishes the principle of direct connection/communication, according to which the competent law enforcement authorities of non-EU Member States cooperate, as would be the case with the EIO. For the collection of electronic evidence, a law enforcement authority in one EU Member State directly requests a warrant from a private sector service provider, which, as Tosza (2022, p.4) argues, does not have the powers to exercise crime prevention, but which is obliged to take a proactive role in the "*prima facie*, the validity and legitimacy of these requests" by cooperating with the law enforcement authorities. In this regard, Mitsilegas (2018, pp.264–265) critically observes that this mechanism leads to the privatization of mutual trust in the field of European criminal justice, since the role of the private sector in the criminal process cannot in any way be assimilated to the powers of the law enforcement authority of the Member State. Here we cannot talk about the effective implementation of control, supervision, and responsibility functions, because the national law enforcement institution and the private sector service provider are two incomparable entities.

Thirdly, unlike the EIO, the EPO mechanism does not provide for a specific procedure for the recognition of an order submitted to an executing authority, including mandatory and optional grounds for non-recognition, etc. Various literary sources indicate that "one may question whether there is still any recognition since there is no authority to actively recognize the order" (Böse 2018). In addition, "the EPO focuses much more on the relationship between

the authorities seeking electronic evidence and the service providers having it. This aspect creates a major difference between the two systems. The EPO goes in the first place to the service provider who should respond to it by delivering the requested data without engaging local authorities who could exercise some checking function from the perspective of national interest or fundamental rights" (Tosza 2020, p.177).

Fourthly, as regards EPOs and European Preservation Orders, these orders can only be issued and presented to the issuing authority, i.e., the service provider, to obtain data held by them. The mechanism of operation of these orders, unlike in the case of EIOs, does not allow the service provider to collect data that are not yet available at the time the order is being submitted. This aspect, among other things, has been criticized in the literature (Laurits 2020, p.70), as the limitations of the Regulation when it comes to obliging the service provider to collect electronic evidence in real time fundamentally undermine the effectiveness of this legal regulation.

Fifthly, there is a difference in the level of protection of the safeguards for the parties involved in the proceedings: in the case of a EPO, the service provider, as a private sector entity – unlike in the case of an EIO, where the order is recognized and executed by the law enforcement authorities of the executing State – will not look at the possible constraints on the interests of the parties to the proceedings and their safeguards "with public eye, they will do so with the private one. In other words, business interests will guide these assessments: what is more profitable, comply with the order or resist?" (Tosza 2020, p.178). Corhay (2021, p.471) pointed out in this regard that, among other things, the EU institutions still have to evaluate and resolve an extremely sensitive issue which has given rise to significant debate, i.e., whether service providers act within the limits of their respective activities and their powers that they exercise for the protection of fundamental human rights in the field. This problem is also highlighted by Rojszczak (2022, p.1023) as well as Smuha (2018, p.104), according to whom the existing provisions of the Regulation cover only those means of remedies that the suspect or the accused person can effectively exercise after the issuance of an EPO or European Preservation Order. The regulation does not provide an explicit answer as to whether remedies can be used during the process of the issuance of these orders. In addition, it is worth remembering Mitsilegas' (2018, p.264) statement on this point: if the Regulation does not foresee that the issued order must first be checked and investigated by a competent law enforcement (judicial) institution, it is difficult to talk about the effective protection of rights.

In conclusion, it appears that the principal provisions of the Regulation on cross-border access to electronic evidence are seen in a different light concerning

mutual recognition as a guiding force for cooperation. Although the conceptual load of the "guiding force" principle remains the same as in the conclusions of the special EU Summit meeting in Tampere, the needs of Member States to obtain evidence in criminal proceedings located in another State, in particular electronic evidence, change the ways of thinking regarding the effectiveness of judicial cooperation. The aforementioned Regulation creates: new criteria for effective cooperation, i.e., direct connections/communication; the replacement of the law enforcement institution of another EU Member State (executive State) with a private sector entity, which is a service provider; a decrease in the number of grounds for refusal to execute orders, etc. It must be acknowledged that when analyzing the provisions of the Regulation, it was not possible to find convincing arguments in the sources of the doctrine as to why the mechanism of evidence collection established by the Regulation could not be enshrined appropriately in the EIO Directive. After all, the scope of requested electronic evidence determined by the Regulation is quite limited, i.e., only evidence that already exists can be requested. Meanwhile, a request for the collection of electronic evidence in real time can only be granted by the assistance provided by the EIO Directive. It can be assumed that this is a crucial moment which causes discussion about the diversity of the legal regulation of evidence collection in the field of criminal justice within the EU. Some authors (Brière 2021, pp.496–497, 509) even question whether it is generally true that within the EU criminal justice area there has been little discussion so far about the development of a different model that can also enhance the implementation of the principle of mutual recognition – namely, the introduction of the requirement to comply with the common procedural standards. The emergence of such common procedural standards would at least allow the fragmentation of the laws on criminal procedure which regulate judicial cooperation in the field of evidence collection within the EU Member States to be avoided. Furthermore, the fact that the analyzed regulatory framework is not established in a Directive but in a Regulation, which is binding in all its elements and directly applicable in the Member States (on the justification of direct application of the Regulation, see also in that regard the following cases: 34/73 *Variola* [1973] ECR I-981; 93/71 *Leonensio* [1972] ECR I-287), does not in itself reinforce the belief that electronic evidence obtained under the Regulation will be admitted as sufficient evidence in the national courts of the Member States without undue difficulty.

On that point, one can only completely agree with the notions provided in the doctrine. For example, emphasizing the issue of the recognition of electronic evidence in judicial cooperation, Rojszczak writes (2022, p.1001) that "in the case of electronic evidence, the reliability of information is obviously of fundamental

importance, not least because digital data are particularly susceptible to modification, from direct manipulation to actual erasure. As contamination of electronic data is often irreversible, it is particularly important to maintain an appropriate work regime at each stage of collecting and processing digital evidence." At the same time, the author raises specific issues of concern "the question of the permissible use of electronic evidence transferred." The author rightly notes that

> the basic purpose of data transfer is their use in ongoing criminal proceedings. In practice, however, law enforcement agencies not only need electronic evidence during pretrial proceedings (in personam phase) but also during early investigation – to determine whether a crime has been committed (*in rem* phase). In this case, aside from proving the guilt of a defendant, electronic evidence helps to establish the circumstances of the case – and thus to clarify whether further proceedings are necessary. The cross-border transmission of electronic evidence to be used during in rem investigation is controversial, as – in the absence of appropriate safeguards – it may deprive the data subject of a possible judicial review of the measures taken. Ongoing investigations do not necessarily lead to criminal charges being brought, and as a result, the evidence obtained may never be presented to a court (Rojszczak 2022, p.1004).

The Issue of the Admissibility of Electronic Evidence

As has already been mentioned, the issue of recognizing electronic evidence obtained by the procedure established by the Regulation as admissible in the national court of an EU Member State is one of the essential elements that make up the essence of the effective operation of the principle of mutual recognition. In general, the issue of the admissibility of evidence obtained in the field of judicial cooperation is not only a matter of mutual trust and the stability and accountability of national criminal justice across the Member States, but also cross-border criminal justice across EU Member States. After all, it is obvious that mutual legal assistance *sensu largo* mechanisms operating based on mutual recognition in the field of EU law and justice emerge from a single mission: the effective operation of the criminal justice process across the EU Member States in investigating and examining criminal cases and enforcing crime prevention. The same is true of the provisions of the Regulation and the EIO Directive governing the collection of electronic evidence. Indeed, both of the aforementioned legal acts set rather different standards for the form of taking such evidence. This is based, first of all, on the fact that the provisions of the Regulation are intended for the operative collection of electronic evidence stored by the service provider (Article 3(8) of the Regulation) in order to secure and obtain electronic evidence more quickly and effectively. In the view of the author, such an aspiration in itself is not sufficient and does not justify the electronic evidence

collection model, which, in a certain sense, reduces the degree of reliability of the collected evidence. Herein, perhaps, lies the essential assumption of the issue of the admissibility of electronic evidence: if the EIO Directive, which in principle also allows for the real-time collection of electronic evidence as well as the collection of existing evidence, sets a relatively high standard for the collection of such evidence (an established system of recognition of orders, non-recognition and the abundance of grounds for non-execution, the possibility of choosing alternative means of investigation, etc.), the provisions of the Regulation appear to lower this standard quite significantly. This standard is lowered to collect only that evidence which is already stored at the time of receiving EPO or European Preservation Order certificates, i.e., existing electronic data.

Thus, both of the aforementioned legal mechanisms, combined with the principle of mutual recognition, undoubtedly seem to ensure that national courts can avoid any concerns about the unreliability of data collected in the territory of another Member State, and at the same time assuage concerns regarding the effectiveness of mutual recognition and compliance with the principles of gathering such evidence. The mutual recognition criterion is considered "a justification to EU action in the field of criminal procedure" (Öberg 2020, p.59). As Liakopolous (2020, p.347) states, mutual recognition "and therefore the direct 'circulation' between the authorities of the judicial measures, marks the abandonment of the conventional assistance system, based on the slow and cumbersome rogatory mechanism, and is based on mutual trust between the member states, thus presupposing respect for the principles of the rule of law." According to another author, Insa (2007, pp.287–288), "principles related to the effectiveness, usefulness, and legitimacy play a relevant role in the different European legislations. The need for obtaining evidence, the transparency while gathering it, and the respect for freedom of expression are principles reflected in the standards in Europe, but they have a secondary position as far as the admissibility of evidence is concerned. The principles that affect electronic evidence are basically the respect for data protection standards and the respect for the secrecy of communications and the right of freedom of expression."

Even though the Regulation is applicable only as of August 18, 2026, it is already possible to critically assess the fact that some of the principal provisions of the Regulation cast doubt on the reliability of evidence obtained from a service provider which offers services within the territory of the Union and is established in another Member State or, if not established, is represented by a legal representative in another Member State. At this point, it should be noted that only a few insights are presented below, which indicate clearly that the method of direct inquiry/communication established by the Regulation (direct contact

of a Member State's law enforcement authority with a private sector entity that is a service provider or its representative) in criminal justice inadvertently causes doubts as to whether the chosen model of collecting electronic evidence is appropriate.

Firstly, Article 8(1) of the Regulation establishes that – not in all cases, but only when the aim is to access traffic data, except data requested only to determine the identity of the user or obtain content data – the issuing law enforcement authority of the Member State shall notify not only the addressee, i.e., the service provider or their representative, but also the institution ensuring enforcement (the authority in the enforcing State, which, following the national law of that State, is competent to receive an EPO and an EPOC or a European Preservation Order and an EPOC-PR transmitted by the issuing authority for notification or enforcement following this Regulation). This provision is directly related to the grounds for refusal to execute the EPO established in Article 12 of the Regulation. In other words, the grounds for refusal to execute the EPO established in Article 12(1) of the Regulation are assessed only if a notification about an EPO was delivered not only to the service provider (or their representative), but also to the enforcement authority of the Member State that received that order. Accordingly, as provided for in Article 12(2) of the Regulation, where the enforcing authority raises a ground for refusal under paragraph 1, it shall inform the addressee and the issuing authority. The addressee shall stop the execution of the EPO and not transfer the data, and the issuing authority shall withdraw the order.

This raises a discussion question as to why the provisions of the Regulation on the one hand segregate electronic data/evidence for which the notice regarding the EPO is issued to both the service provider (or their representative) and the enforcement authority, while for other electronic evidence, such as subscriber data, the EPO is addressed to the private sector entity, i.e., the service provider, only. On the other hand, there is no clear answer as to the question of why the grounds for refusal to execute an EPO are only examined if the enforcement authority also receives notification regarding this order, which means that in the case of the collection of subscriber data, the grounds for refusal will not be examined. Therefore, could the grounds for refusing to execute the order, i.e., the contradiction to the principle of *ne bis in idem*, be relevant in seeking to obtain electronic evidence of subscriber data (Article 3(9) of the Regulation)? The existing legal framework, when compared with the principal provisions of the EIO Directive, suggests that the mechanism created by the Regulation for the collection of existing (stored) electronic evidence provides for a substantially more liberal approach, which does not necessarily ensure the same standard of protection of human rights as the EIO Directive does.

Secondly, to maintain consistency and an optimum level of confidence in decisions taken in terms of judicial cooperation with another EU Member State, the grounds for refusal to execute an EIO, as set out in Article 12(1) of the Regulation, should, if not identical to those set out in Article 11(1)(c) of the EIO Directive, at least be approximate to those set out in Article 11(1). Particular attention should be drawn to Article 11(1)(b) of said Directive: in a specific case, the execution of the EIO would harm essential national security interests, jeopardize the source of information or involve the use of classified information relating to specific intelligence activities. The uniform or at least similar and systematically harmonized introduction of the above grounds for non-recognition or non-execution in EU criminal justice legislation would enable the avoidance of excessive heterogeneity and non-uniformity of the legal requirements (standards of procedural form). The harmonization of the regulatory framework (in particular the EIO Directive and the Regulation) would not only bring more legal clarity and legal certainty, but would also enhance confidence in the EU legal system. Trust in the EU legal system, accordingly, leads to the "free movement" of evidence, especially electronic evidence, across EU Member States.

Thirdly, an important issue that needs to be addressed is the admissibility of electronic evidence. However, the Regulation is silent on the procedures for recording, storing, and transferring the data stored by the service provider for which the order was issued, which may differ due to differences in territorial jurisdiction across EU Member States. Thus, even though the Regulation allows the collection of preexisting stored data only, it must therefore be held that this does not change anything in substance. Both the gathering of evidence in real-time (in the case of the application of the EIO Directive) and the process of collecting data at the time of the submission of the order should be subject to uniform provisions or, as is well chosen in the case of the EIO mechanism, the order should specify the procedural steps (methods) by which such electronic evidence should be collected, stored, recorded, and transmitted to the State that issued the order (for example, Article 5(1)(e) of the EIO Directive). Unfortunately, however, unlike in the EIO Directive, the Regulation does not contain any rules or provisions concerning this issue, which in turn may create grounds for raising doubts in a national court regarding the assessment of the admissibility of electronic evidence collected following the Regulation.

Concluding on this point, it should be noted that the model of electronic evidence collection chosen by the Regulation does not indisputably prevent discussions on the obstacles to recognizing such evidence as admissible in the national court of a Member State. The existing regulatory framework, which could indeed have been more coherent and at the same time at least minimally

aligned with the model set out in the EIO Directive, has not avoided fragmentation. The aforementioned fragmentation, as well as the differentiation of the evidence collection process within the framework of EU criminal justice, could be reduced via the *Doctrine of Common Minimum Standards* proposed by some authors (Kusak 2017, p.349; Depauw 2016, p.98). According to this doctrine, all EU legal instruments that accelerate and assist Member States in cooperating in the investigation and prosecution of criminal offenses must contain at least minimum common standards to ensure uniformity in, for example, the gathering of evidence on a case-by-case basis, especially when it comes to the use of expert investigations (Depauw, 2016, p.98), procedural safeguards, the use of the same procedural form, the observance of identical principles, etc. According to the literature, the "gathering of evidence under commonly agreed minimum standards would make it easier for an issuing state to accept the way that the evidence is being gathered in the executing state. Therefore, the idea of common EU minimum standards has the potential to accommodate the problem of mutual admissibility of evidence in criminal matters in the EU" (Kusak 2017, p.349). A thorough analysis of this doctrine would, of course, require a separate study; however, it is already possible to assert that the issue of the admissibility of electronic evidence is not addressed by the provisions of the Regulation either.

Interim Findings

After unlimited efforts to look for an optimized EU criminal justice model in the context of "free movement of evidence," in 2023 Regulation (EU) 2023/1543 of the European Parliament and of the Council on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings was adopted. This legal regulation, it would seem, should have solved the problems related to the challenges that electronic data collection issues are subject to in the EU. The background to the Regulation and the paradigm of the legislative process show that the bodies involved in the legislative process – the EU Member States – sought to give a different impetus to the collection of electronic evidence than to the collection of other evidence. The aim was not only to have a fast, efficient data collection process, but also to develop a model of electronic evidence collection that would allow the law enforcement authorities of the Member States to avoid mutual contact with the law enforcement authorities of other countries, and instead to establish direct contact with the addressees, i.e., service providers (or their representatives). The parallel of this model would seem to allow the electronic evidence stored to be grasped and collected as quickly as possible.

Unfortunately, an analysis of the existing regulatory framework for the gathering of evidence (including electronic evidence) (EIO, Regulation on the Taking of Electronic Evidence) suggests that the Regulation, in order to ensure the timely and efficient gathering of evidence, lacks provisions ensuring the admissibility of such evidence before national courts.

The provisions of the Regulation on the taking of electronic evidence are characterized by their fragmentary nature, which is the result of a lack of certain safeguards that are particularly emphasized in legal practice. In particular, the selective nature of the process of refusal to recognize and execute orders for the production of electronic evidence, the lack of safeguards for the rights of the individual, the lack of procedural guarantees, and the specificity of the process of collecting, recording, and transmitting electronic evidence stored by a private body (a service provider) all mean that the admissibility of such evidence in national courts may be seriously called into question.

To avoid obstacles to the admissibility of electronic evidence collected outside the territory of the national State in which the trial is taking place, it was necessary to bring the principal provisions of the Regulation in line with those of the Directive regarding the EIO in criminal matters. At the same time, it should be emphasized that other measures have also been proposed in the academic literature that could assist in reducing the fragmentation, fundamental inconsistency, and excessive heterogeneity concerning the legal instruments of criminal justice within the EU. These include the application of the doctrine of *Common Minimum Standards* to all legal instruments on judicial cooperation without any exception.

References

Abraha, H. H., 2020. Regulating Law Enforcement Access to Electronic Evidence Across Borders: The United States Approach. *Information and Communications Technology Law*, 29 (3), 324–353.

Belevičius, L., 2013. Tarptautinis teisinis bendradarbiavimas ir Europos Sąjungos baudžiamasis procesas: aktualijos, perspektyvos, lūkesčiai [International Legal Cooperation and Criminal Proceedings of the European Union: Current Affairs, Perspectives, Expectations]. In: *Baudžiamojo proceso tarptautiškumas: patirtis ir iššūkiai.* Vilnius: Mykolo Romerio Universitetas, 170–209.

Blažič, B. J., and Klobučar, T., 2020. Investigating Crime in an Interconnected Society: Will the New and Updated EU Judicial Environment Remove the Barriers to Justice? *International Review of Law, Computers and Technology*, 34 (1), 87–107.

Böse, M., 2018. *An Assessment of the Commission's Proposals on Electronic Evidence* [online]. European Parliament. Available from: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf [Accessed 8 August 2023].

Brière, C., 2021. EU Criminal Procedural Law onto the Global Stage: The E-Evidence Proposals and Their Interaction With International Developments. *European Papers*, 6 (1), 493–511. Available from: https://doi.org/10.15166/2499-8249/479 [Accessed 14 August 2023].

Consolidated Version of the Treaty on the Functioning of the European Union [online]. *Official Journal*, C326. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012E/TXT [Accessed 8 August 2023].

Corhay, M., 2021. Private Life, Personal Data Protection and the Role of Service Providers: The EU E-Evidence Proposal. *European Papers*, 6 (1), 441–472. Available from: https://doi.org/10.15166/2499-8249/477 [Accessed 14 August 2023].

Corhay, M., 2023a. *It is a Long Way to … E-Evidence: EU Reforms in the Collection of Electronic Evidence – Part 1* [online]. Information Law and Policy Centre. Available from: https://infolawcentre.blogs.sas.ac.uk/2023/01/24/it-is-a-long-way-to-e-evidence-eu-reforms-in-the-collection-of-electronic-evidence-part-1/ [Accessed 25 July 2023].

Corhay, M., 2023b. *It is a Long Way to… E-Evidence: EU Reforms in the Collection of Electronic Evidence Part 2 – The Role of Service Providers* [online]. Available from: https://infolawcentre.blogs.sas.ac.uk/2023/02/26/it-is-a-long-way-to-e-evidence-eu-reforms-in-the-collection-of-electronic-evidence-part-2-the-role-of-service-providers/ [Accessed 27 July 2023].

Depauw, S., 2016. A European Evidence (Air)Space? Taking Cross-Border Legal Admissibility of Forensic Evidence to a Higher Level. *European Criminal Law Review*, 6 (1), 82–98.

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters [online]. *Official Journal*, L130. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041 [Accessed 30 July 2023].

European Commission Proposal for a regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters. COM/2018/225 final – 2018/0108 (COD), 2018 [online]. *EUR-Lex*. Available from: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM%3A2018%3A225%3AFIN [Accessed 27 July 2023].

European Digital Rights, 2023. *E-Evidence compromise blows a hole in fundamental rights safeguards*' [online]. Available from: https://edri.org/our-work/e-evidence-compromise-blows-a-hole-in-fundamental-rights-safeguards/ [Accessed 27 July 2023].

Insa, F., 2007. The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting Against High-Tech Crime – Results of a European Study. *Journal of Digital Forensic Practice*, 1 (4), 285–289.

Jurka, R., 2011. Tarptautinis bendradarbiavimas baudžiamajame procese: įrodymai ir jų priimtinumas Europos Sąjungoje [International Cooperation in the Criminal Process: Evidence and its Admissibility in the European Union]. In: *Baudžiamasis procesas: nuo teorijos iki įrodinėjimo (prof. dr. Eugenijaus Palskio atminimui)*. Vilnius: Mykolo Romerio universitetas, 89–128.

Jurka, R., 2019. Įrodymų perdavimo Europos Sąjungos valstybių narių baudžiamojoje justicijoje iššūkiai ir atradimai [Challenges and Innovations of Evidence Transfer in European Union Member States' Criminal Justice]. *Jurisprudencija*, 26 (2), 308–325.

Kosta, E., and Kamara, I., 2023. The Right to an Effective Remedy in International Data Transfers of Electronic Evidence: Past Lessons and Future Outlook. *Review of European Administration Law*, 16 (1), 57–83.

Kusak, M., 2017. Common EU Minimum Standards for Enhancing Mutual Admissibility of Evidence Gathered in Criminal Matters. *European Journal on Criminal Policy*, 23, 337–352. https://doi.org/10.1007/s10610-017-9339-0 [Accessed 30 July 2023].

Kusak, M., 2019. Mutual Admissibility of Evidence and the European Investigation Order: Aspirations Lost in Reality. *ERA Forum*, 19, 391–400. Available from: https://doi.org/10.1007/s12027-018-0537-0 [Accessed 30 July 2023].

Laurits, E., 2020. Regulating the Unregulatable: an Estonian Perspective on the CLOUD Act and the E-Evidence Proposal. *Juridica International*, 29, 62–70.

Leroux, O., 2004. Legal Admissibility of Electronic Evidence. *International Review of Law Computers*, 18 (2), 193–220.

Liakopoulos, D., 2020. Mutual Recognition and Criminal Efficiency under Regulation (EU) 2018/1805 for the Mutual Recognition of Freezing and Confiscation Measures. *International Criminal Law Review*, 20, 346–370.

Mangiaracina, A., 2014. A New and Controversial Scenario in the Gathering of Evidence at the European Level: The Proposal for a Directive on the European Investigation Order. *Utrecht Law Review*, 10 (1), 113–133.

Mitsilegas, V., 2018. The Privatisation of Mutual Trust in Europe's Area of Criminal Justice: The Case of E-evidence. *Maastricht Journal of European and Comparative Law*, 25 (3), 263–265.

Öberg, J., 2020. Trust in the Law? Mutual Recognition as a Justification to Domestic Criminal Procedure. *European Constitutional Law Review*, 16, 33–62.

Petri, A., 2018. *No Law Enforcement by Private Corporations* [online]. Available from: https://www.telekom.com/en/company/management-unplugged/details/no-law-enforcement-by-private-corporations-544132 [Accessed 30 July 2023].

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 [online]. *Official Journal*, L191, 118–180. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1543 [Accessed 8 August 2023].

Rojszczak, M., 2020. CLOUD Act Agreements from an EU Perspective. *Computer Law and Security Review*, 38, 105442.

Rojszczak, M., 2022. E-Evidence Cooperation in Criminal Matters from an EU Perspective. *The Modern Law Review*, 85 (4), 997–1028.

Smuha, N. A., 2018. Towards the EU harmonization of Access to Cross-Border E-evidence: Challenges Fundamental Rights & Consistency. *European Criminal Law Review*, 8 (1), 83–115.

Tosza, S., 2020. 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*, 11 (2), 161–183.

Tosza, S., 2022. The Public Role of Private Actors: Internet Service Providers in the E-Evidence Proposal [online]. *European Law Blog* [blog], 22 September 2022. Available from: https://europeanlawblog.eu/2022/09/20/the-public-role-of-private-actors-internet-service-providers-in-the-e-evidence-proposal/ [Accessed 12 August 2023].

Warken, C., van Zwieten, L., and Svantesson, D., 2020. Re-thinking the Cooperation of Data in the Context of Law Enforcement Cross-Border Access of Evidence. *International Review of Law, Computers and Technology*, 34(1), 44–64.

Jolanta Zajančkauskienė / Rima Ažubalytė /
Oleg Fedosiuk (eds.)

Towards Coherence in Criminal Justice

Challenges, Discussions And/Or Solutions

PETER LANG

Berlin - Bruxelles - Chennai - Lausanne - New York - Oxford

Library of Congress Cataloging-in-Publication Data

Names: Zajančkauskienė, Jolanta, editor. | Ažubalytė, Rima, editor. | Fedosiuk, Oleg, editor.
Title: Towards coherence in criminal justice : challenges, discussions, and/or solutions / edited by Jolanta Zajančkauskienė, Rima Ažubalytė, and Oleg Fedosiuk.
Description: New York : Peter Lang, 2025. | Includes bibliographical references and index.
Identifiers: LCCN 2025015805 (print) | LCCN 2025015806 (ebook) | ISBN 9783631929445 (hardcover) | ISBN 9783631935323 (ebook) | ISBN 9783631935330 (epub)
Subjects: LCSH: Criminal justice, Administration of. | Criminal jurisdiction. | Criminal law. | Criminal liability. | Evidence, Criminal. | Electronic evidence. | Convention for the Protection of Human Rights and Fundamental Freedoms (1950 November 5) | Fair trial.
Classification: LCC K5001 .T69 2025 (print) | LCC K5001 (ebook) | DDC 345—dc23/eng/20250403
LC record available at https://lccn.loc.gov/2025015805
LC ebook record available at https://lccn.loc.gov/2025015806

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek collects this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at .Nationalbibliografie; detailed bibliographic data are available on the Internet at http://dnb.d-nb.de.

Mykolas Romeris University

Reviewers:
Prof. dr. Edita Gruodytė (Vytautas Magnus University, Lithuania)
Prof. dr. hab. Wieslaw Plywaczewski (University of Warmia and Mazur in Olsztyn, Poland)

Copy-editor:
MB "Kopis"

Approved by Mykolas Romeris University Law School Council on 11 of June 2024 by resolution No. 1T-14 (1.12 E-20401).

ISBN 978-3-631-92944-5 (Print)
ISBN 978-3-631-93532-3 (E-PDF)
ISBN 978-3-631-93533-0 (E-PUB)
DOI.10.3726/b22750

Published by Peter Lang GmbH, Berlin, Germany
info@peterlang.com - www.peterlang.com

Contents