A new EU system on cross-border gathering of e-evidence – analysis and open questions

*Anže Erbežnik**

ABSTRACT

The article outlines a significant shift in the approach to international cooperation ain criminal law on electronic evidence (e-evidence). The EU's e-evidence package, proposed in 2018, introduces a framework where Member States can directly request electronic evidence from service providers in other Member States. This bypasses traditional mutual legal assistance channels and raises questions about sovereignty, territoriality, and human rights protections, especially in relation to privacy and data protection. The initial proposal of the e-evidence package was met with various amendments from the EU Council and Parliament, focusing on extra-territoriality, notification procedures, and safeguarding fundamental rights. The final legislation shows certain elements of these perspectives but largely aligns with the Commission and Council's vision. It emphasizes cooperation between public judicial authorities and private service providers, blurring the lines between public and private sectors. This raises concerns about outsourcing fundamental rights protection to the private sector. Such an approach lacks the necessary fundamentals, namely certain common standards, illustrated on the examples of data retention and admissibility of evidence. The EU Court of Justice has challenged general and indiscriminate data retention practices, advocating for targeted retention to combat serious crimes, under strict conditions to protect personal data and privacy rights. The disparity in data retention approaches reflects varying national attitudes towards privacy across the EU. The admissibility of cross-border evidence is also a complex is-

* Prof. of Criminal Law and Criminal Procedure (European Law Faculty, Slovenia) and Advisor in the EP Committee on Legal Affairs. Opinions expressed in this text are personal opinions of the author.

sue, given the differing legal standards and procedures among EU Member States. The EU has not established a unified framework for this. This situation leads to potential legal conflicts and challenges in ensuring the rights of the accused are protected in cross-border cases. In conclusion, the e-evidence system marks a significant shift in cross-border legal cooperation within the EU. While it addresses the need for efficient access to electronic evidence in a digital age, it also raises profound questions about the balance between effective law enforcement and the protection of fundamental rights in an era of increasingly pervasive digital surveillance. The system's potential to undermine privacy and data protection standards, both within the EU and in international relations, warrants careful consideration and ongoing scrutiny.

Keywords: e-evidence, electronic evidence, data retention, mutual recognition in criminal law, admissibility of evidence, EU criminal law

Nov sistem EU za čezmejno zbiranje elektronskih dokazov (e-dokazov) – analiza in odprta vprašanja

POVZETEK

Članek opisuje pomemben premik v pristopu k mednarodnemu sodelovanju v kazenskem pravu glede elektronskih dokazov (e-dokazov). Paket e-dokazov EU, predlagan leta 2018, uvaja okvir, v katerem lahko države članice neposredno zahtevajo elektronske dokaze od ponudnikov storitev v drugih državah članicah. To obide tradicionalne kanale medsebojne pravne pomoči in odpira vprašanja o suverenosti, teritorialnosti in zaščiti človekovih pravic, še posebej v zvezi z zasebnostjo in zaščito osebnih podatkov. Začetni predlog paketa e-dokazov je bil deležen različnih dopolnil s strani Sveta EU in Evropskega parlamenta, ki so se osredotočili na ekstrateritorialnost, postopke obveščanja in varovanje temeljnih pravic. Končna zakonodaja obsega določene elemente teh pomislekov, vendar se v veliki meri usklajuje z vizijo Evropske komisije in Sveta EU. Poudarja sodelovanje med javnimi pravosodnimi organi in zasebnimi ponudniki storitev, kar briše mejo med

javnim in zasebnim sektorjem. Tak pristop neposrednih odredb nima potrebnih temeljev, zlasti nekaterih skupnih standardov, kar je prikazano na primerih hrambe podatkov in dopustnosti dokazov. Sodišče EU je izpodbijalo prakse splošnega in nediskriminatornega hranjenja podatkov, zagovarjajoč ciljno usmerjeno hrambo za boj proti resnim kaznivim dejanjem, pod strogimi pogoji za zaščito osebnih podatkov in pravic do zasebnosti. Raznolikost pristopov k hrambi podatkov odraža različna nacionalna stališča do zasebnosti po vsej EU. Dopustnost čezmejnih dokazov je prav tako kompleksno vprašanje, glede na različne pravne standarde in postopke med državami članicami EU. Sana EU še ni vzpostavila enotnega okvira za to. To vodi do morebitnih pravnih sporov in izzivov pri zagotavljanju pravic obdolženih v čezmejnih primerih. Skratka, sistem e-dokazov označuje pomemben premik v čezmejnem pravnem sodelovanju znotraj EU. Čeprav naslavlja potrebo po učinkovitem dostopu do elektronskih dokazov v digitalni dobi, prav tako odpira poglobljena vprašanja o ravnovesju med učinkovitim kazenskim pregonom in zaščito temeljnih pravic v dobi vseprisotnega digitalnega nadzora. Potencial sistema za spodkopavanje standardov zasebnosti in zaščite podatkov, tako znotraj EU kot v mednarodnih odnosih, zahteva skrbni premislek.

Ključne besede: e-dokazi, elektronski dokazi, hramba podatkov, medsebojno priznavanje v kazenskem pravu, sprejemljivost dokazov, kazensko pravo EU

1. Introduction

Due to the development of technology and the need for rapid cooperation, as well as the risk of electronic evidence (e-evidence) being deleted and the increasing emphasis on cross-border elements in obtaining such evidence, the Commission proposed in 2018 an instrument that radically changes the previous way of understanding mutual recognition and cooperation, namely the so-called »e-evidence« package.[1] With it, the Commission introduces a kind of all-European order that is issued by one Member State and directly addressed to a private provider of electronic services in another Member State. At the

[1] See further Carrera, 2020; Tosza, 2018, pp. 212–219; Tosza, 2020, pp. 161–183; Christakis, 2020; Bonačić, 2021, pp. 123–140; Tinoco-Pastrana, 2020, pp. 46-50; Corhay, 2021, pp. 441-471; Erbežnik, Dežman, 2022, pp. 432-441.

same time, there is an obligation to appoint a special representative for operators from third countries that do not have an establishment in the EU. The package consists of two legislative texts, namely a regulation, (Regulation (EU) 2023/1543, 2023, p. 118) which is based on mutual recognition in criminal law (Art. 82 of the Treaty on the Functioning of the European Union (TFEU)), and a directive, (Directive (EU) 2023/1544, 2023, p. 181) which harmonises provisions of laws or other regulations in Member States concerning the establishment and provision of services (Art. 53 and Art. 62 TFEU). Such logic stands for a trend in EU law allowing direct contacts between judicial authorities from one Member State and private providers from another, without the involvement of the executing/enforcing state's authority, and granting certain public powers to private providers (e.g. assessment of human rights violations).[2] At the same time, it introduces extraterritorial application of law and thus redefines national territoriality and sovereignty of Member States and third states by allowing interference with human rights without the knowledge of the state on whose territory the provider is located, and without the possibility of its objection. In some countries, there is already a trend of extending national orders to other countries.[3] In parallel, the Second additional protocol to the Council of Europe's Budapest Cybercrime Convention has been adopted[4] and an agreement with

[2] See Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online (OJ L 172, 17.5.2021, p. 79) based on Art. 114 TFEU (internal market). It introduces direct contacts between authorities in one Member State and service providers in another one to remove or disable access to terrorist content online in all Member States within one hour, with the optional possibility of subsequent review by the Member State where the hosting service provider has its main establishment or where its legal representative is located. In doing so, it is assessed whether there is a serious or manifest infringement of the regulation or of fundamental rights and freedoms guaranteed by the EU Charter of Fundamental Rights (Charter). The same logic is also applied in Regulation (EU) 2022/2065 on a Single Market For Digital Services (OJ L 277, 27. 10. 2022, p. 1).

[3] For example, consider the so-called US Cloud Act (US Clarifying Lawful Overseas Use of Data Act), which amended the Electronic Communications Privacy Act (ECPA). It was passed as a result of the *US v. Microsoft* case, 584 U.S._ (2018), concerning the question of whether the ECPA allowed US law enforcement authorities to compel a provider located in the US to disclose the contents of data stored outside the US (email stored in Ireland). See also the Belgium Skype and Yahoo cases in view of a broad interpretation of national orders – see de Hert, 2018, pp. 1-27.

[4] Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence (CETS No. 224). Even prior to the Protocol attempts have been made to resolve the issue of direct access through interpretation of Art. 18(1)(b) of the Cybercrime Convention with regard to the requirement for a service provider on its territory to provide data on subscribers in relation to services it provides. See Cybercrime Convention Committee, 2017. The relevant issue is also addressed to a limited extent in Art. 32 of the Cybercrime Convention, provided that the person who has valid authorisation to disclose the data agrees, or when the data is publicly accessible. See also Council Decision (EU) 2023/436 authorising Member States to ratify, in the interest of the European

the United States on the direct acquisition of electronic data is taking place.[5]

However, such a novel approach can be problematic from the perspective of extremely different standards of human rights protection (especially on the right to privacy and personal data protection) when obtaining e-evidence, both between EU Member States and as regards third states (such as signatories to the Cybercrime Convention, including Turkey, Sri Lanka, Philippines, etc.).[6] Essential differences exist, for example, in the authority that approves gathering of e-evidence, the required level of suspicion, proportionality and the types of offences for which such measures can be requested, rules on admissibility of evidence, general data retention obligations by providers, etc. Such a system also substantially interferes with fundamental rights protection obligations on one's own territory under the ECHR system.[7] At the same time, there is a difference in the application between the two proposals that form the e-evidence package. While the directive binds all Member States, this does not apply to the regulation. Consequently, the directive shows a plan for the use of the concept of legal representation more broadly, also in other instruments, as a general trend of public-private cooperation in the prosecution of criminal offences. Additionally, it underestimates the sensitivity of e-evidence in the technological age providing extensive insight into privacy of an individual (full picture of one's private life). In that regard this article will firstly, compare

Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (OJ L 63, 28. 2. 2023, p. 48).

[5] Council decision authorising the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters. Council EU, doc. 10128/19.

[6] A good example is the pending CJEU EncroChat case C-670/22, *Staatsanwaltschaft Berlin*, whereby evidence gathered legally in France based on minimum standards is being spread to other Member States although there such evidence could not have been legally obtained due to stricter requirements.

[7] During a public hearing regarding the e-evidence proposal in the European Parliament on 27 November 2018, EctHR Judge Bošnjak highlighted that the law of the executing state does not seem relevant within the framework of the proposal. From the perspective of the Convention, this could cause problems, as the high contracting parties to the European Convention on Human Rights (ECHR), including all EU Member States, are responsible for protecting human rights on their territory. They must establish a regulatory framework and provide legal, if not judicial, protection in individual cases. If a complaint is submitted to the bodies of the executing state, they cannot refrain from investigating the complaint by merely stating that they are implementing EU legislation. This was clearly stated in the ECtHR *Avotiņš v. Latvia* judgment. According to Judge Bošnjak the proposal, in terms of ECtHR case law, created a relatively unique situation. Interferences with Art. 8 ECHR do not include the bodies of the executing state. It is questionable whether this is in line with ECHR. Legitimate expectations could arise that the law of the executing state would be applied in every case, which would affect the assessment of legality. See European Parliament, 3rd Working document, 2019.

the initial Commission e-evidence proposal with the final legislative instrument agreed; secondly, evaluate the proposal in view of extra-territoriality; thirdly, provide an assessment of such a system in view of fundamental differences on data retention; and fourthly and lastly, present the Slovenian national doctrine on evaluation and admissibility of cross-border evidence.

2. The EU e-evidence system

2.1. The original proposal and response to it

In its original proposal[8] the Commission envisaged a system whereby a judicial authority from one Member State would in criminal proceedings[9] directly turn to a provider of electronic communication services in the Union, which has an establishment or representative in another Member State, for the submission or preservation of e-evidence, without involving the executing/enforcing state.[10] This is based on two orders/certificates: the European Production Order Certificate (EPOC)[11] and the European Preservation Order Certificate (EPOC-PR),[12] which are intended for historical electronic data only and not for live (real-time) interception. The Commission proposed initially four categories of electronic data to be covered: (1) subscriber data, (2) access data, (3) transactional data, and (4) content data.[13] Un-

[8] Initial proposal of e-evidence Regulation (COM/2018/225 final).
[9] This also applies to proceedings against legal persons in the issuing state, regardless of the concept of criminal liability of legal persons in the executing state (Art. 3 of the initial proposal).
[10] E-evidence means evidence stored in electronic form by a service provider or stored on their behalf at the time of receipt of a European Production Order or European Preservation Order, including stored data on subscribers, access, transactions, and content (Art. 2(6) of the initial proposal). Unlike traditional mutual recognition under Art. 82 TFEU, the enforcing/executing state does not participate in principle. In this context, different terminology is deliberately used, as the term »executing state« is replaced by »enforcing state.« However, such an extensive interpretation of Art. 82 TFEU is questionable, as the provisions of EU Treaties on criminal law should be narrowly interpreted. This was the view of the German Federal Constitutional Court in its assessment of the Lisbon Treaty (BVerfG, 2 BvE 2/08 *et al.*, 30 June 2009), and was raised by the European parliament during negotiations on the e-evidence package (European Parliament, 2nd Working document, 2019).
[11] A binding decision of the issuing authority of a Member State, requiring the service provider offering services within the Union and established or represented in another Member State, to produce e-evidence (Art. 2, point 1, of the initial proposal).
[12] A binding decision of the issuing authority of a Member State requiring the service provider offering services in the Union and established or represented in another Member State to preserve e-evidence in view of a subsequent request for production (Art. 2, point 2, of the initial proposal).
[13] Data related to the commencement and termination of a user access session to a service, which is strictly necessary for the sole purpose of identifying the user of the service, such as the date and time of use, or the log-in to and log-off from the service, together with the IP address allocated by the internet access service provider to the user of a service, data identifying the interface used and the

like the traditional division as known in national legislations and the Cybercrime Convention (subscriber data, traffic data, content data), a new category of »access data« has been added, with an unclear distinction from traffic/transactional data. However, the division between the different data categories is essential regarding the nature of the issuing authority. A request for traffic/transactional and content data can only be issued or validated by a court, while a request for subscriber and access data as well as for the preservation of all types of data can be issued or validated by either a prosecutor or a court.[14] This division also affects the type of criminal offences for which an order can be issued. An order for the submission of transactional/traffic and content data can only be made for certain specific crimes, namely offences punishable by a penalty of more than three years and certain other specified crimes, while an order for subscriber and access data as well as for preservation can be issued for all offences.[15] The service provider, according to the initial Commission proposal, would have to provide the data within 10 days and in urgent circumstances within 6 hours, or preserve the data for 60 days with the possibility of an extension. The provider could have refused to provide the data only if the certificate was incomplete, contained obvious errors, or did not contain sufficient information, due to force majeure, because compliance is actually impossible, or because it is apparent from the information in the certificate that it violates the EU Charter or that the order is obviously abusive.[16] Only in case of non-disclosure, the issuing state turns to the enforcing state, which is supposed to force the provider to send the data.[17] A special procedure was provided in the event of conflict with third country law.[18] Such a new instrument only complements Directive 2014/41/EU (EIO Directive, 2014, p. 1) on the European Investigation Order (EIO Directive).[19]

---

user ID. This includes electronic communications metadata (Art. 2, point 8, of the initial proposal). Among other things, the Commission has attempted to resolve the issue of dynamic IP addresses, which are traffic data as such, but, by their nature, if they relate to identity, are also similar to subscriber data. However, for both access data and transaction data the Commission added the same statement, namely that "[t]his includes electronic communication metadata".

[14] Art. 4 of the initial proposal.

[15] Art. 5 and Art. 6 of the initial proposal.

[16] Art. 9 and Art. 10 of the initial proposal.

[17] Art. 14 of the initial proposal.

[18] Art. 15 and Art. 16 of the initial proposal.

[19] Art. 23 of the initial proposal.

The EU Council followed suit in its general approach (General approach, 15292/18) with some amendments, expanding the scope to the execution of custodial sentences or detention orders that were not rendered *in absentia* in case the convict absconded from justice, introducing the possibility of subsequent approval by a competent authority in emergency situations, and limiting the review by service providers. (General approach, 15292/18, Art. 3(2) and 4(5)) Furthermore, it introduced a consultation procedure for traffic data in cases that are not considered domestic (non-domestic cases), (General approach, 15292/18, Art. 5(7)) and a very limited notification to the enforcing state authorities regarding content data in non-domestic cases, but without suspensive effect. (General approach, 15292/18, Art. 7a) In that regard the Council tried, at least partially, to address the issue of extra-territoriality in its general approach by distinguishing between "domestic" and "non-domestic" cases. It considered cases to be "domestic" when the suspect is in the issuing state, regardless that the data is in another state. However, the European Parliament (EP) as co-legislator tried to significantly amend the original proposal due to several legal reservations. (Draft report PR1191404SL; EP text for negotiations A9-0256/2020) It introduced in its initial position a significant substantive notification procedure with non-recognition grounds and the possibility of a response from the enforcing state, following the European Investigation Order (EIO) model. In doing so, it differentiated between different procedures for transmitting data according to their invasiveness, namely direct transmission for some data and a notification procedure for more intrusive data requests. It also strengthened the provisions regarding remedies and supplemented them with provisions on admissibility of evidence. The extremely difficult legislative negotiations in trilogues[20] took almost two years under five Council presidencies (started with Portuguese in 2021 and ended with Swedish in 2023), all together eight trilogues.

2.2. The main features of the final e-evidence system

The final e-evidence text (Regulation (EU) 2023/1543, 2023, p. 118) seems to be mainly in line with the visions of the Com-

[20] The author of this text took part during the whole negotiation procedure on e-evidence, as well as its predecessor, the European Investigation Order.

mission and Council, and much less in line with concerns expressed by the EP. Two instruments remained despite the EP's fear that the directive would be used for other purposes (the legal representative). However, through negotiations, this was clearly confirmed, showing a trend where cross-border cooperation is no longer just judicial cooperation, but includes also cooperation between public judicial authorities and private service providers, thereby blurring the lines between private and public and raising serious issues of outsourcing fundamental rights protection to private parties. Further, despite keeping the three classical categories of electronic data, a special place had to be given to IP addresses and similar identifiers called "data requested for the sole purpose of identifying the user". (Regulation (EU) 2023/1543, 2023, Art. 3, point 10 and Art. 4(1)) This means that the final text still left the final denomination of IP addresses and similar notifiers as subscriber or traffic data to national authorities. However, this also means that for such data, a prosecutorial order from the issuing State is possible to be addressed to a provider in an enforcing State where a court order is still necessary (it seems at least in the case of Germany and Slovenia and possibly others). How the national constitutional legal system will react when confronted with such a challenge can only be guessed for the moment. There is only a reference that a court might be included in the notification or enforcing stage if required by national law.[21] In that sense, a possible solution for providers from such Member States would be to oppose prosecutorial orders if a court order is required in their national system, thereby triggering the need for an enforcement procedure. There were also some improvements in view of legal remedies (Regulation (EU) 2023/1543, 2023, Art. 18) and more clarity on the third country law dispute procedure. (Regulation (EU) 2023/1543, 2023, Art. 17) However, the biggest difference of the final text in comparison with the initial proposal relates to notification and non-recognition grounds.

[21] In Recital 61 it is stated that where a notification to the enforcing authority, or enforcement, takes place in accordance with the Regulation, the enforcing State could provide under its national law that the execution of a European Production Order might require the procedural involvement of a court in the enforcing State.

2.2.1. Notification

As regards notification, the final compromise foresees a meaningful notification with refusal grounds only for traffic and content data in »non-domestic« cases. (Regulation (EU) 2023/1543, 2023, Art. 8 and Art. 12) If a case is considered "domestic", no notification takes place. A case is considered as "domestic" if: (a) the offence has been committed, is being committed or is likely to be committed in the issuing State, and (b) the person whose data are sought resides in the issuing State. In the recitals further guidance is provided what is considered "residence". The prime indicator is registration in a Member State. In the absence of such it can be also indicated by the fact that a person has manifested the intention to settle or has acquired following a stable period of presence in that Member State certain connections with that state. As possible objective criteria for assessment family ties, economic connections, registered vehicles, bank accounts are listed. However, it is added that a short visit, holiday stay, including a holiday home, should not be considered enough. (Regulation (EU) 2023/1543, 2023, Rec. 53) The agreed criteria leave certain interpretation space and a possible misuse of the term "domestic" is possible. It is neither clear if this is enough to satisfy the requirements from ECtHR case-law on foreseeability and ECHR territorial protection, even in cases of mutual recognition in EU civil and criminal matters. For example, in *Avotiņš v. Latvia* the ECtHR stated that the court in the State addressed must at least be empowered to conduct a review commensurate with the gravity of any serious allegation of a violation of fundamental rights in the State of origin, in order to ensure that the protection of those rights is not manifestly deficient. (ECtHR, Avotiņš v. Latvia [GC], 2016, para. 114-116)[22] This applies even more so as it is not clear that the Bosphorus (ECtHR, Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi v. Ireland [GC], 2005) presumption of adequacy of EU fundamental rights protection would be satisfied in view of substantial rule of law problems in some Member States amounting even to Art. 7(1) TEU proceedings and confirmed also by ECtHR case-law.[23]

[22] See also ECtHR, *Pirozzi v. Belgium*, a. no. 21055/11, judgment of 17 April 2018, para. 62–64; ECtHR; and *Romeo Castano v. Belgium*, a. no. 8351/17, judgment of 9 July 2019, para. 84. Both cases apply the *Avotiņš* test to mutual recognition in criminal matters in view of European Arrest Warrants.
[23] See ECtHR, *Xero Flor w Polsce sp. z o.o. v. Poland*, a. no. 4907/18, judgment of 7 May 2021, as regards

2.2.2. Fundamental rights non-recognition ground

One of the positive outcomes for the EP was the inclusion of non-recognition grounds in case of notification, whereby the it managed to salvage the most meaningful grounds from the EIO Directive, namely privileges, *ne bis in idem*, double criminality, and fundamental rights. (Regulation (EU) 2023/1543, 2023, Art. 8 and Art. 12) In trilogues, one of the main issues was the nature of certain grounds, namely the question of whether they are obligatory or facultative. Only Council Framework Decision 2002/584/JHA on the European Arrest Warrant (2002, Art. 3 and Art. 4) established such a differentiation, while subsequent mutual recognition instruments, such as EIO, introduced them only as facultative (»may« clause).[24] In the final text of Art. 12(1), the following phrase was used: »shall [...] assess the information [...] and, where appropriate, raise one or more of the following grounds for refusal«. The intention is to reflect that there are cases where the only possible decision is to use a certain ground, despite the fact that the judicial authority always makes the decision. The EP also succeeded to include a fundamental rights non-recognition grounds referring to Art. 6 TEU. Such an inclusion, as already part of the EIO, is essential in view of possible higher national constitutional standards. In view of the mediocre solution in some EU harmonisation directives on procedural rights setting very law standards (especially the right to a lawyer), this is essential. Furthermore, the EP managed to keep the classical double criminality understanding outside the category of 32 offences. The Commission wanted an expansion of the list to hate speech, which would, without a common EU definition, trigger serious issues in view of the different national understanding of the topic.

In the past one of the main questions in EU criminal law was how to formulate a fundamental rights non-recognition clause. What is clear is that the clause is broader than »flagrant denial of justice,« the ECtHR concept regarding the absence of fundamental elements of a fair trial that prevents extradition. (Guide on Art.

---

the illegality of composition of the Polish Constitutional Court. See also a whole variety of CJEU judgments on the independence of judiciary in Poland – cases C-619/18, C-585/18, C-624/18 in C-625/18, C-204/21, etc. There are also proceedings based on Art. 7(1) TEU against Hungary and Poland.

[24] However, the Commission is introducing again the distinction between obligatory and facultative non-recognition grounds in Art. 13 of the Proposed regulation on the transfer of proceedings in criminal matters (COM/2023/185 final).

6 (criminal limb), 2020, pp. 101–102)[25] From the perspective of the uniform application of EU law, it is not legally sound that in different EU criminal law instruments and CJEU judgments different clauses are used. Thus, some Member States, which have introduced a special national non-recognition ground for human rights violations, refer to Art. 6 TEU, such as the Austrian law, which states, »if there are objective circumstances that the judgment was a result of the violation of fundamental rights or fundamental legal principles within the meaning of Art. 6 TEU«. (EU-JZG, 2004, Art. 40, Pt. 12) In Council Framework Decision 2005/214/JHA on mutual recognition of financial penalties, (2005, p. 16) the »reason to believe that fundamental rights or fundamental legal principles of the Treaty have been violated under Art. 6 of the Treaty« is used. (Framework Decision 2005/214/JHA 2005, At. 20(3)) In the past, the EP advocated a clause referring to Art. 6 TEU, thus stating three levels of human rights protection, namely ECHR, EU Charter, and constitutional traditions common to the Member States. The latter category is essential to prevent »Solange« conflicts between EU law and national constitutions. Through a reference to Art. 6 the EU legislature gives national judicial authorities the possibility to consider higher national constitutional standards in certain cases. Such a clause was used in the EIO Directive, stating that »there are substantial grounds to believe that the execution of the investigative measure provided for in the EIO would be incompatible with the executing state's obligations under Art. 6 TEU and the Charter«. (EIO Directive, 2014, Art. 11(1)(f))

In contrast, Regulation (EU) 2018/1805 (2018, p.1) on mutual recognition of freezing and confiscation orders uses a more restrictive version stating that »in exceptional situations, there are substantial grounds to believe, on the basis of specific and objective evidence, that the execution of the freezing order would, in the particular circumstances of the case, entail a manifest breach of a relevant fundamental right as set out in the Charter, in particular the right to an effective remedy, the right to a fair trial or the right of defence«. (Regulation (EU) 1805/2018, 2018, Art. 8(1)(f)

[25] See also ECtHR, *Soering v. United Kingdom*, a. no. 14038/88, judgment of 7 July 1989, para. 113; *Mamatkulov and Askarov v. Turkey* [GC], a. no. 46827/99 in 46951/99, judgment of 4 February 2005, para. 90 and 91; *Al-Saadoon and Mufdhi v. United Kingdom*, a. no. 61498/08, judgment of 2 March 2010, para. 149.

and Art. 19(1)(h)) Further, the CJEU has set its own standards and a two-step test in cases of *Aranyosi* (CJEU, joined cases C-404/15 and C-659/15 PPU) and *LM,* (CJEU, case C-216/18) namely "whether there are substantial grounds to believe that the individual concerned by a European arrest warrant, issued for the purposes of conducting a criminal prosecution or executing a custodial sentence, will be exposed, because of the conditions for his detention in the issuing Member State, to a real risk of inhuman or degrading treatment" or "where that authority finds, after carrying out a specific and precise assessment of the particular case, that there are substantial grounds for believing that the person in respect of whom that European arrest warrant has been issued will, following his surrender to the issuing judicial authority, run a real risk of breach of his fundamental right to an independent tribunal and, therefore, of the essence of his fundamental right to a fair trial". The displayed »cacophony« of human rights clauses could cause confusion. It is not practical, realistic and legally sound that Member States anticipate such different clauses for each instrument when transposing and applying EU law. From a practical standpoint, the fundamental question is only whether there is a risk of a violation or not. Consequently, harmonization of the different existing clauses is necessary.

2.2.3. Emergency cases

However, the EP acknowledged in view of notification a special case in "emergency cases" defined as situations in which there is threat to the life, physical integrity or safety of a person, or to a critical infrastructure, where the disruption or destruction of such critical infrastructure would result in an imminent threat to the life, physical integrity or safety of a person through a serious harm to the provision of basic supplies to the population or the exercise of the core functions of the State. (Regulation (EU) 2023/1543, 2023, Art. 3, pt. 18) In such cases, a 8-hour deadline is foreseen (in comparison with the usual 10 days) and in "non-domestic" cases for traffic and content data only an ex-post notification takes place. In that regard the enforcing state may in 96 hours object to the use of such data and demand its deletion or agree to its use under certain circumstances. (Regulation (EU) 2023/1543, 2023, Art. 10(4)) Such a solution has been inspired by

Art. 31(3)(b) of the EIO Directive dealing with cross-border wiretappings without the technical assistance of the executing state. The indicated definition of emergency cases leaves a lot or leverage to the issuing State, thus diminishing the limited meaningful notification system even further. The result is farfetched from the initial safeguards demanded by the EP. In addition, one of the main problems of operating the envisaged e-evidence system is the lack of harmonisation at EU level of basic notions on the collection and use of electronic data, such as data retention and the issue of admissibility of cross-border evidence.

3. Lack of uniformity on data retention among EU Member States

The diversity of approaches among EU Member States on data retention shows the different attitude towards privacy and protection of electronic data in the EU. Data retention refers to the mandatory retention of traffic telecommunications data for a certain period for all individuals, based on the possibility of future use in criminal proceedings. This is the logic of the so-called preventive state, which is also reflected in other EU instruments regarding the mass collection of data on individuals, profiling, and cross-linking of various data sources. Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (2006) introduced an obligation for Member States to prescribe mandatory retention of traffic telecommunications data ranging from six months to two years. However, the way to access this data was entirely left to national authorities.[26] The CJEU declared the directive invalid in the *Digital Rights Ireland* (CJEU, joined cases C-293/12 and C-594/12) case for violating Art. 7 and Art. 8 of the EU Charter, i.e., the protection of privacy and personal data. It noted that the directive applies even to persons for whom there is no indication that their conduct might have a link, even an indirect one, with serious crime, and that it is not limited to the retention of data in relation to a period and/or a particular geographic area and/or a

[26] In Slovenia, the relevant directive was transposed with the Electronic Communications Act (ZEKom-A and ZEKom-1). The legislation was annulled by the Slovenian Constitutional Court, No. U-I-65/13, 3 July 2014.

group of individuals, that might be linked in one way or another to a serious crime, or solely to data of persons who could, for other reasons, contribute, by the mere fact that their data are being retained, to the prevention, detection or prosecution of serious offenses. (CJEU, joined cases C-293/12 and C-594/12, para. 58 and 59) The absence of procedural and substantive conditions for access by national authorities was also highlighted in the *Tele2/Watson* (CJEU, joined cases C-203/15 in C-698/15) case. The CJEU declared that general national systems on data retention that remained in force after the *Digital Rights Ireland* case were incompatible with EU Treaties, Directive 2002/58/EC and the EU Charter. It thus prohibited the general and indiscriminate retention of all traffic data and location data for all subscribers and registered users of all electronic communications means, stating that such a system allowed very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the daily habits, places of permanent or temporary residence, daily or other movements, activities, social relationships and the social environments frequented by those persons. It stated that that this "is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance". (CJEU, joined cases C-203/15 in C-698/15, para. 99 and 100) However, it allowed targeted retention of traffic and location data to combat serious crime, if the retention of data regarding the categories of stored data, the communication means used, the persons involved, and the duration of the relevant retention is limited to what is strictly necessary, and if the national regulations are based on clear and precise rules that regulate the scope and use of such data retention measures and that establish minimum requirements, so that persons whose data has been retained have sufficient guarantees enabling them to effectively protect their personal data against the risks of abuse. Similarly, several national constitutional courts followed the same logic. (See Zubik et al., 2021; Fennelly, 2019, pp. 673–692)

However, at least half of Member States have maintained dana retention system and the Commission has not initiated proceedings for a violation of EU law, where appropriate. It seems that also the CJEU has succumbed to pressure from law enforcement agencies and has partly retracted from the original strict prohibition of general retention system. In the *Ministerio Fiscal* (CJEU,

case C-207/16) case, the issue was narrowed down only to access to already stored data and it was allowed to access identification data of SIM card holders activated with a stolen mobile phone, such as name, surname, and if necessary, address of the holders, for all criminal offences and not just for fighting serious crime. In the *Privacy International* (CJEU, case C-623/17) and La *Quadrature du Net et al.* (CJEU, joined cases C-511/18, C-512/18 and C-520/18) cases, the CJEU confirmed the validity of EU law on data protection in the field of national security. (CJEU, joined cases C-511/18, C-512/18 and C-520/18, para. 87–104)[27] However, it allowed for the possibility of a general retention system regarding subscriber data and IP addresses, targeted retention of location and traffic data, and for exceptions to the prohibition of general and indiscriminate retention of such data. Thus, in the case of a serious threat to national security, which proves to be real and present or foreseeable, a system was allowed whereby providers of electronic communications services are required to store data on traffic and location generally and indiscriminately, and the decision on such an order may be subject to effective supervision by a court or independent administrative body whose decision is binding to verify the existence of one of these situations and compliance with the conditions and guarantees that must be specified, and the said decision may be issued only for a period that is limited to what is strictly necessary, but in the event of the continued existence of this threat, it may be extended. (CJEU, joined cases C-511/18, C-512/18 and C-520/18, para. 134–139) With regard to the protection of national security, the fight against serious crime and the prevention of serious threats to public security, a Member State may also adopt rules for targeted retention of traffic and location data on a preventive basis, provided that such retention is limited to what is strictly necessary in terms of categories of stored data, communication means covered, persons concerned and the duration of retention. Such a limitation may be based on the category of persons as well as on a geographical criterion, where competent national authorities, based on objective and nondiscriminatory elements, consider that there is a situation characterized by a high risk of preparation or commission of serious criminal offences in one or more geographical areas. (CJEU,

[27] See also newer judgments based on the same principles referring to the German (joined cases C793/19 and C794/19, *SpaceNet and Telekom*) and Irish systems (case C140/20, *Garda Síochána*).

joined cases C-511/18, C-512/18 and C-520/18, para. 140–151)

Similarly, for the protection of national security, the fight against serious crime and the prevention of serious threats to public security, for a period limited to what is strictly necessary, general and indiscriminate retention of IP addresses assigned to the connection source, as well as general and indiscriminate retention of data on the civil identity of users of electronic communication tools, is permissible. (CJEU, joined cases C-511/18, C-512/18 and C-520/18, para. 152–159) Automated analysis and real-time collection are also allowed within certain limits. However, in that regard the CJEU touched upon admissibility rules. While acknowledging national autonomy in that regard, it nevertheless stated that EU law „requires national criminal courts to disregard information and evidence obtained by means of the general and indiscriminate retention of traffic and location data in breach of EU law, in the context of criminal proceedings against persons suspected of having committed criminal offences, where those persons are not in a position to comment effectively on that information and that evidence and they pertain to a field of which the judges have no knowledge and are likely to have a preponderant influence on the findings of fact". ((CJEU, joined cases C-511/18, C-512/18 and C-520/18, para. 221–228) In the case of *H.K.*, (CJEU, case C-746/18) it repeated the aforementioned rules on admissibility and at the same time denied the possibility of granting direct access to traffic and location data to a prosecutor. Such a body can only be a judicial or other independent body, i.e. a body that has all the powers and guarantees necessary to reconcile the various relevant interests and rights. With regard to criminal investigations, this court or body must ensure a fair balance between the interests related to the needs of the investigation, which concern the fight against crime, on the one hand, and the fundamental rights to respect for private life and the protection of personal data of individuals, to whose data access is granted, on the other. If this review is not carried out by a court, but by an independent administrative body, that body must have a status that allows it to act objectively and impartially in the performance of its tasks, and must be protected from any external influence for this purpose. Furthermore, the body responsible for this preliminary review, first, does not participate in the investigation of the relevant criminal offences, and second, is neutral with respect to

the parties in the criminal proceedings. This does not apply to the state prosecution, which directs the investigation and, if necessary, represents the prosecution, since the task of the state prosecution is not to decide the dispute completely independently, but to submit the dispute to the competent court, as a party to the proceedings, which represents the prosecution. (CJEU, case C-746/18, para. 52–59) Such CJEU judgments can be understood as the beginning of EU law on the admissibility of evidence (*in statu nascendi*).

4. Cross-border admissibility of evidence

A complex legal question is the question of admissibility of evidence obtained abroad, which is a mirror image of the issue of foreign requests. The question of admissibility of evidence or their exclusion is directly related to the fundamental rights of the defendant in criminal proceedings. Therefore, this question is often a constitutional question. At the same time, exclusionary rules are a matter of legal culture and generations of lawyers are trained to respect these standards. Their respect is also related to the perception of the legitimacy of a particular legal system. (Erbežnik, 2014, pp. 131-152) The question of preserving national standards of admissibility of evidence, which are directly related to some fundamental constitutional guarantees (such as the requirement for judicial approval for some measures), is often a question of preserving the standards of one's own constitution in proceedings before national courts. Cross-border cooperation bears the danger of *forum shopping*, where systems with the least safeguards are sought and evidence is obtained there, which is then transferred (for example, within the framework of a joint investigation team).[28] At the same time, there is also a risk of transplanting foreign anomalies to your own system (for example, the absence of the need for a judicial order for invasive measures into privacy). In practice, the following questions are often raised: the nature of the body that obtained the evidence abroad, the territorial validity of the national constitution, the definition of fundamental constitutional and international principles of protection of the rights of the accused, and effective legal remedies.

[28] See ft. 6.

Based on the above, three different approaches to the issue of evidence obtained abroad are possible: (a) mutual recognition of evidence (goods theory), (b) adherence to the provisions of national criminal proceedings or (c) allowing evidence if they are in accordance with fundamental constitutional and international principles of protection of individual rights in criminal proceedings. (Alegrezza, 2010, pp. 569–579) Solutions (a) and (b) are unrealistic extremes and only solution (c) seems reasonable. The assessment of admissibility of evidence is currently exclusively a national jurisdiction of EU Member States, as there are no common EU rules yet.[29] Directive 2013/48/EU on the right of access to a lawyer (2013, Art. 12(2))[30] and Directive 2016/343/EU on the presumption of innocence indicate some beginnings in view of reference to "defence rights and fairness of proceedings". Therefore, the issues related to evidential rules in the sense of the *Melloni* (CJEU, case C-399/11) case are currently not arising (the issue of minimum common EU standards and the disregard of higher national constitutional standards).[31] This means that the question of admissibility of evidence is left to national constitutional and legal orders. In the original proposal for a regulation on the European Public Prosecutor's Office (Proposal COM(2013) 534 final, 2013) the European Commission attempted to introduce automatic acceptance and circulation of evidence obtained by the European Public Prosecutor's Office in another EU Member State if the fairness criteria was met and are only for criminal proceedings of the European Public Prosecutor. (Proposal COM(2013) 534 final, 2013, Art. 30(1))[32] However, this approach received nu-

[29] However, there is a proposal from the European Law Institute on a Directive of the European Parliament and the Council on Mutual Admissibility of Evidence and Electronic Evidence in Criminal Proceedings, 2023 (https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Proposal_for_a_Directive_on_Mutual_Admissibility_of_Evidence_and_Electronic_Evidence_in_Criminal_Proceedings_in_the_EU.pdf).

[30] "Member States, without prejudice to national rules and systems concerning the admissibility of evidence, ensure that, in the context of criminal proceedings, the rights of the defense and the fairness of the proceedings are respected when evaluating statements made by suspects or accused persons or evidence obtained in violation of their right to a lawyer or in cases where derogation from that right was permitted in accordance with Art. 3(6)."

[31] It seems that first steps in view of EU admissibility rules stem from CJEU judgments- see case C-746/18, *H.K.*, *supra,* where the court emphasizes the importance of adversarial proceedings in challenging evidence. Further, it also required in principle a court authorisation for traffic data.

[32] "Evidence presented by the European Public Prosecutor's Office to the trial court, where the court considers that its admission would not adversely affect the fairness of the procedure or the rights of defence as enshrined in Art. 47 and Art. 48 of the Charter of Fundamental Rights of the European Union, shall be admitted in the trial without any validation or similar legal process even if the national law of the Member State where the court is located provides for different rules on the collection or presentation of such evidence."

merous criticisms and was not adopted in the final version of Regulation (EU) 2017/1939.[33]

4.1. Nature of the authority that orders investigative measures

The issue of asymmetry between ordering authorities is one of the fundamental questions in the implementation of mutual legal assistance and mutual recognition, and the question arises in view of requesting authorities that are not judicial authorities. Instruments at the level of the Council of Europe and the EU left the determination of the »judicial authority« to the discretion of each state.[34] However, newer EU mutual recognition instruments are moving towards introducing a special validation procedure by a prosecutor or court in the ordering state in case of non-judicial authorities, while also problematizing the asymmetry between Member States regarding the role of the prosecutors. Judicial review of certain criminal law measures is the result of an important recognition of the potential danger of abuses by law enforcement. As a result, in a vast majority of democratic states measures such as house searches or other intrusions into privacy require in principle a judicial authorisation. In the era of modern technology, the internet, and consequently new modern technological possibilities available to law enforcement agencies, the demand for judicial authorisation is becoming increasingly important and even essential for the effective protection of reasonably expected privacy.

But judicial control should not be merely a formality, but a substantive critical evaluation within a reasonable time frame. As already mentioned, there has been a question of different attitudes towards judicial review. Thus, the definition of »judicial authority« was left to issuing Member States, some of which consider ministries and police to be judicial authorities, as shown in relation to the European Arrest Warrant.[35] Certain harmonisation has recent-

[33] The proposed standard of »fairness of proceedings« might have been too low compared to ECtHR case-law regarding evidence obtained through torture, inhuman or degrading treatment (Art. 3 ECHR), for example, ECtHR, *Gäfgen v. Germany*, *Othman (Abu Qatada) v. United Kingdom*, and *El Haski v. Belgium*. Regarding admissibility of evidence and EPPO, the European Parliament proposed in its report a different approach, namely a clause referring to Art. 6 TEU (similar to Directive 2014/41/EU). See European Parliament, Interim Report of 24 February 2014 on the proposal for a Council Regulation on the establishment of the European Public Prosecutor's Office, P7_*TA(2014)0234.*

[34] *For example, Art. 24 of the CoE 1959 MLA Convention or Art. 6 of Framework Decision 2002/584/JHA on the European Arrest Warrant.*

[35] *For example, CJEU, case C-452/16 PPU, Poltorak, judgment of 10 November 2016; CJEU, case*

ly emerged from CJEU as regards data retention as mentioned before. The problem of granting judicial powers to the police in certain Member States was first addressed in Framework Decision 2008/978/JHA on the European Evidence Warrant, (2008) by establishing a specific refusal ground (see Art. 11(4) and (5) in conjunction with Art. 13 of Framework Decision 2008/978/JHA). This was more comprehensively addressed and resolved in the aforementioned EIO Directive by introducing a validation procedure in the issuing state. (2014, Art. 2(c)(ii))[36] In addition, the mentioned Directive introduced also the possibility of judicial approval in the executing state to prevent asymmetrical situations as regards prosecutors. (Art. 2, pt. d)[37] The aim was to prevent, for example, a state prosecutor from the issuing state, where a search warrant can be issued by him or her, from directly addressing a request to the police in the executing state, where a court order is required. Therefore, the aim was to prevent a conflict between mutual recognition on the one hand and national (constitutional) standards on the other hand in terms of protecting higher national (constitutional) standards. This issue is also mirrored in relation to the admissibility of evidence obtained in another state, although the EIO Directive does not address the admissibility of evidence issue. However, the e-evidence system disregards this solution and provides for a possibility of prosecutors requesting data on a territory of a Members State where a court order is necessary for such data. An automatic acceptance of requests submitted by a non-judicial body, without a prior judicial order in the issuing country, could be problematic if the national constitution requires court approval. This is because court approval can be a fundamental part of a national constitutional arrangement in

C-453/16, Özcelik*, judgment of 10 November 2016; CJEU, case C-477/16 PPU, Kovalkovas, judgment of 10 November 2016.*

[36] "Issuing authority' means: (i) a judge, a court, an investigating judge or a public prosecutor competent in the case concerned; or (ii) any other competent authority as defined by the issuing State which, in the specific case, is acting in its capacity as an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law. In addition, before it is transmitted to the executing authority the EIO shall be validated, after examination of its conformity with the conditions for issuing an EIO under this Directive, in particular the conditions set out in Art. 6(1), by a judge, court, investigating judge or a public prosecutor in the issuing State. Where the EIO has been validated by a judicial authority, that authority may also be regarded as an issuing authority for the purposes of transmission of the EIO."

[37] "'executing authority' means an authority having competence to recognise an EIO and ensure its execution in accordance with this Directive and the procedures applicable in a similar domestic case. Such procedures may require a court authorisation in the executing State where provided by its national law."

criminal proceedings, based on past experiences and recognition of possible abuses.

4.2. Fundamental rights of the accused in criminal proceedings and a 4-step theory to assess admissibility of cross-border evidence

Based on a similar approach of the Slovenian Supreme Court[38] and the Constitutional Court[39] the author of this article proposes that admissibility of evidence obtained abroad should be assessed at four levels of cascading verification: - respect for the rules in the country of acquisition; - minimum ECHR rules ;[40] - minimum EU rules (EU Charter of Fundamental Rights and directives on the rights of the suspect or accused);[41] - possible higher national con-

[38] For example, Slovenian Supreme Court, No. Kp 16/2007, 30 May 2008.

[39] Cross-border evidence is admissible in Slovenia if it has been obtained in accordance with foreign procedural law and if it has not been obtained in violation of constitutionally guaranteed human rights and fundamental freedoms. The Constitutional Court held that when an individual claims that evidence obtained abroad is unconstitutional and should therefore be excluded from the case, the court must first clearly define the upper premise of the evaluation of the alleged accusations. Only when this legal basis is established, can the court assess the admissibility and usability of evidence obtained abroad and make a further assessment of whether the ruling may rely on such evidence. This means comparing the foreign legal system from the perspective of the ECHR as well as the Slovenian Constitution. However, it seems that in later case-law the court is limiting the assessment only to certain procedural safeguards of the Slovenian Constitution, not necessarily including the right to privacy. See Slovenian Constitutional Court, No. Up-519/12, 18 September 2014; Slovenian Constitutional Court, No. Up-995/15, 12 July 2018 and Slovenian Constitutional Court, No. Up-899/16, Up-900/16 and Up-901/16, 5 May 2022.

[40] Evidence that violates Art. 3 ECHR shall be prohibited and there shall be a strong presumption of inadmissibility of evidence obtained by violating essential elements of Art. 6 and Art. 8 ECHR. For example, in the ECtHR cases of Heino v. Finland (no. 56720/09) and Harju v. Finland (no. 56716/09) regarding safeguards for house searches. This should also apply to the collection of criminal data by intelligence services without appropriate safeguards, especially if there is ECtHR case law against the relevant state (for example, Ekimdzhiev v. Bulgaria, no. 62540/00, judgment of 28 June 2007, on the legislation for implementing special measures), denial of the right to a lawyer during police interrogations (for example, Salduz v. Turkey [GC], no. 36391/02, judgment of 27 November 2008, on the right to a lawyer during police interrogations, which also triggered legislative changes in EU countries, or Panovits v. Cyprus, no. 4268/04, judgment of 11 December 2008, on the need to be informed about the right to a lawyer in certain circumstances), and violations of the right to remain silent (for example, Heaney and McGuinness v. Ireland or Saunders v. United Kingdom). The criminal procedure is an organic entity, and allowing evidence that does not meet even the minimum standard of the ECHR contaminates the entire chain of evidence (especially if the remaining evidence directly relies on such evidence, but also more broadly - it is not clear, for example, whether someone testifies because the inadmissible evidence is already in the file, or independently of it). In that regard also the exclusionary rule should be respected (including the fruit of the poisonous tree doctrine).

[41] If this is not met, then there should be at least a strong presumption that such evidence is not admissible. See, for example, directives from the so-called Roadmap on the fundamental rights of the accused in criminal proceedings. These acts establish a »federal minimum« within the EU in relation to the catalogue of rights from the EU Charter of Fundamental Rights. It is interesting to compare this with the United States, where achieving the federal minimum from the Bill of Rights does not prevent stricter procedural rules in the states. This means that evidence that does not meet the federal minimum is always inadmissible. The admissibility of evidence that meets the federal minimum in one state but not in another with stricter rules depends on its assessment, and is therefore not auto-

stitutional standards. However, the last criterion is the most problematic and requires more caution as it is not possible to impose the national procedural safeguards and standards automatically on other countries.[42] For example, the requirement for the presence of two witnesses during an investigative act does not mean that only evidence from countries that also require the presence of two witnesses is admissible, but the essence is that the other system also prevents arbitrariness. The assessment of proportionality through a limitation to catalogue criminal offences should be understood in a similar way. It is not necessary for the same acts to be listed in both countries if both take proportionality into account when ordering such measures. At the same time, it is necessary to distinguish between the constitutional core and the statutory extension of a particular interpretation of a right.

5. Conclusions

The EU e-evidence system was proposed and adopted based on a new ideology of cross-border orders disregarding the classical limits in view of national sovereignty. To a certain extent, this is understandable in view of cases where it is not clear where data is. However, pretending in clear-cut cases that the data is "domestic" stretches established legal concepts and safeguards in cross-border cooperation immensely. As one of the authors correctly put it, we would need a new international "Lotus"[43] case providing clear international guidance on cross-border encroachments of another's sovereignty. This is even more so in an age where e-evidence is becoming the main evidence, and all our lives are stored or can be traced electronically. Consequently, it seems that the executive branches, legislators, and many judges are underestimating the seriousness of this new approach. It also shows a certain decline in general political and legal sensitivity

matic. See Ouwerkerk,, 2011, pp. 206-210. Similarly, within the EU, national constitutions can provide for higher standards than those at the common level, and the question of the primacy of EU law over national constitutions has never been fully resolved, see the "Solange doctrine", taking into account Art. 4 TEU (respect for national identity).

[42] See also the on-going project of the European Law Institute on Fundamental Constitutional Principles to identify and articulate the fundamental constitutional principles which form the foundations of European constitutionalism.

[43] De Hert, ft. 3. The Lotus refers to a landmark case in front of Permanent Court of International Justice (PCIJ), the predecessor to the International Court of Justice (ICJ), decided in 1927. The case arose from a collision between two ships in the high seas. It established the principle that a state may act as it wishes so long as it does not contravene an explicit prohibition.

to privacy and data protection in the technological age. Direct orders are problematic also inside the EU as a kind of "race to the bottom", with the lowest common denominators prevailing, and considering rule of law problems in several EU Member States. At least for EU Member States it might have been easier to use a more evolutionary approach amending the European Investigation Order, adding a new chapter on e-evidence.[44] They are even more problematic from an international perspective, whereby the EU is conducting negotiations with third states despite significant differences in data protection rules, understanding of privacy, the problems with death penalty, etc. Time will tell if the critical reservations towards a new system were justified However, if they were, it will be very difficult to »put the genie back into the bottle« as shown in similar cases in the past, e.g., data retention.

Keywords: e-evidence, electronic evidence, data retention, mutual recognition in criminal law, admissibility of evidence, EU criminal law

BIBLIOGRAPHY AND SOURCES

Articles

Alegrezza, S., Critical Remarks on the Green Paper on Obtaining Evidence in Criminal Matters from one Member State to another and Securing its Admissibility, Zeitschrift für Internationale Strafrechtsdogmatik, Vol. 5, št. 9/2010, str. 569–579

Bonačić, M., Pristup elektroničkim dokazima: na putu prema novom modelu kaznenopravne suradnje u EU, Hrvatska akademija znanosti i umjetnosti, 2021, pp. 123–140

Christakis, T., E-Evidence in the EU Parliament: Basic Features of Birgit Sippel's Draft Report, European Law Blog, 2020

Corhay, M., Private Life, Personal Data Protection and the Role of Service Providers: the EU e-Evidence Proposal, European Papers, Vol. 6, No. 1(2021), pp. 441-471

Cybercrime Convention Committee, T-CY Guidance Note No. 10, Production orders for subscriber information (Article 18 Budapest Convention), 2017

De Hert, P., et. al., New Journal of European Criminal Law, Vol. 9, No. 3(2018), pp. 1-27

Tinoco-Pastrana, A., The Proposal on Electronic Evidence in the European Union, eurocrim, No. 1/2020, pp. 46-50

Carrera, S., et al., Cross-border data access in criminal proceedings and the future of digital justice, CEPS. 2020

Erbežnik, A. (2014). Mutual Recognition in EU Criminal Law and Its Effects on the Role of a National Judge. In: Peršak, N. et al., Legitimacy and Trust in Criminal Law, Policy and Justice, Ashgate.

Erbežnik, A., Dežman, Z. (2022). Uvod v kazensko procesno pravo RS in EU, Ljubljana: GV Založba.

European Parliament, 2nd Working document on the proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (2018/0108 (COD)) - Scope of application and relation with other instruments, DT\1176230EN, 6 February 2019. URL: https://www.europarl.europa.eu/doceo/document/LIBE-DT-634729_EN.pdf.

European Parliament, 3rd working document on the proposal for a regulation on the European Production and Preservation Order and the European Preservation Order for electronic evidence in criminal matters (2018/0108 (COD)) - implementation of EPO and EPR in practice and the role

[44] *Whereby Ireland is* not participating in the EIO but is participating in e-evidence.

of service providers, DT_1177089EN, 13 February 2019. URL: https://www.europarl.europa.eu/RegData/commissions/libe/document_travail/2019/634849/LIBE_DT(2019)634849_EN.pdf
Fennelly, D., Data retention: the life, death and afterlife of a directive, ERA Forum 19 (2019), pp. 673–692.
Tosza, S., (2018). The European Commission's Proposal on Cross-Border Access to E-Evidence, eucrim, No. 4/2018, pp. 212–219.
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, Vol. 11, No. 2/2020, pp. 161–183.
Zubik, M., et al., (2021). European Constitutional Courts towards Data Retention Laws, Springer.

Jurisprudence

BVerfG, 2 BvE 2/08 et al., 30 June 2009
CJEU, case C-399/11, Melloni, judgment of 26 February 2013.
CJEU, joined cases C-293/12 and C-594/12, Digital Rights Ireland and Kärntner Landesregierung et al., judgment of 8 April 2014.
CJEU, joined cases C-404/15 and C-659/15 PPU, Aranyosi and Căldăraru, judgment of 5 April 2016.
CJEU, case C-452/16 PPU, Poltorak, judgment of 10 November 2016;
CJEU, case C-453/16, Özcelik, judgment of 10 November 2016;
CJEU, case C-477/16 PPU, Kovalkovas, judgment of 10 November 2016
CJEU, case C-216/18, LM, judgment of 25 July 2018.
CJEU, joined cases C-203/15 in C-698/15, Tele2 Sverige and Watson, judgment of 21 December 2016
CJEU, case C-207/16, Ministerio Fiscal, judgment of 2 October 2018
CJEU, case C-623/17, Privacy International, judgment of 6 October 2020
CJEU, joined cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net et al., judgment of 6 October 2020
CJEU, joined cases C793/19 and C794/19, SpaceNet and Telekom, judgment of 20 Semptember 2022
CJEU EncroChat case C-670/22, Staatsanwaltschaft Berlin, pendingECtHR, Al-Saadoon and Mufdhi v. United Kingdom, a. no. 61498/08, judgment of 2 March 2010
ECtHR, Avotiņš v. Latvia [GC], a. no. 17502/07, judgment of 23 May 2016.
ECtHR, Bosphorus Hava Yolları Turizm ve Ticaret Anonim Şirketi v. Ireland [GC], a. no. 45036/98, judgment of 30 June 2005.
ECtHR, Ekimdzhiev v. Bulgaria, no. 62540/00, 28 June 2007
ECtHR, Mamatkulov and Askarov v. Turkey [GC], a. no. 46827/99 in 46951/99, judgment of 4 February 2005
ECtHR, Panovits v. Cyprus, no. 4268/04, judgment of 11 December 2008
ECtHR, Pirozzi v. Belgium, a. no. 21055/11, judgment of 17 April 2018
ECtHR, Romeo Castano v. Belgium, a. no. 8351/17, judgment of 9 July 2019
ECtHR, Salduz v. Turkey [GC], no. 36391/02, judgment of 27 November 2008
ECtHR, Soering v. United Kingdom, a. no. 14038/88, judgment of 7 July 1989
ECtHR, Xero Flor w Polsce sp. z o.o. v. Poland, a. no. 4907/18, judgment of 7 May 2021
Slovenian Supreme Court, No. Kp 16/2007, 30 May 2008
Slovenian Constitutional Court, No. Up-519/12, 18 September 2014
Slovenian Constitutional Court, No. Up-995/15, 12 July 2018
Slovenian Constitutional Court, No. Up-899/16, Up-900/16 and Up-901/16, 5 May 2022
Slovenian Constitutional Court, No. U-I-65/13, 3 July 2014.

Legal sources

Directive (EU) 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, pp. 54–63. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2006:105:FULL, 24.10.2023.
Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty, OJ L 294, 6.11.2013, pp. 1–12. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0048, 24.10.2023.
Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying

down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings – e-evidence Directive, OJ L 191, 28.7.2023. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023L1544, 23.10.2023.

EIO Directive, Directive 2014/41/EU, OJ L 130, 1.5.2014. URL : https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0041, 23.10.2023.

EP text for negotiations, A9-0256/2020. URL: https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_EN.html#_section2, 23.10.2023.

EU-JZG, 2004. Bundesgesetz über die justizielle Zusammenarbeit in Strafsachen mit den Mitgliedstaaten der Europ.ischen Union (BGBl. I Nr. 36/2004). URL : https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2004_I_36/BGBLA_2004_I_36.pdfsig, 23.10.2023.

Framework Decision 2002/584/JHA, COUNCIL FRAMEWORK DECISION of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States, OJ L 190, 18.7.2002. URL: https://eur-lex.europa.eu/resource.html?uri=cellar:3b151647-772d-48b0-ad8c-0e4c78804c2e.0004.02/DOC_1&format=PDF, 23.10.2023.

Framework Decision 2005/2145/JHA, COUNCIL FRAMEWORK DECISION 2005/214/JHA of 24 February 2005 on the application of the principle of mutual recognition to financial penalties, OJ L 76, 22.3.2005. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2005:076:FULL, 23.10.2023.

Framework Decision 2008/978/JHA, COUNCIL FRAMEWORK DECISION 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters, OJ L 350, 30.12.2008. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2008:350:FULL.

General approach, 15292/18. Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters. URL: https://data.consilium.europa.eu/doc/document/ST-15292-2018-INIT/en/pdf, 23.10.2023.

Guide on Art. 6 (criminal limb), Council of Europe, 2020, str. 101–102. URL: https://www.echr.coe.int/documents/d/echr/guide_art_6_criminal_eng, 23.10.2023.

Proposal COM(2013) 534 final, Proposal for a COUNCIL REGULATION on the establishment of the European Public Prosecutor‘s Office, 17.7.2013. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0534:FIN:en:PDF, 24.10.2023.

Proposal COM(2018) 225 final, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for electronic evidence in criminal matters, 17.4.2018. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN.

REGULATION (EU) 2018/1805 of the European Parliament and of the Council of 14 November 2018 on the mutual recognition of freezing orders and confiscation orders, OJ L 303, 28.11.2018. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2018:303:FULL, 23.10.2023.

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 – e--evidence Regulation, OJ L 91, 28.7.2023. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R1543, 23.10.2023.