Ariadna H. Ochnio, Hanna Kuczyńska (eds),
Current Issues of EU Criminal Law
(Publishing House of ILS PAS 2022)
DOI: 10.5281/zenodo.6856038
pp. 73–88

Mutual trust to obtain electronic evidence in the EU: is the bar low or high?

Martyna Kusak

Abstract

The European Union is in urgent need of a specific, streamlined mechanism for the preservation and production procedures for electronic data stored by service providers. This is needed in order to accelerate the cross-border obtainment of such data and relieve the pressure on the mutual assistance system used in relations with non-EU states. Hence, in 2018, the European Union launched a proposal for electronic evidence gathering which introduced rules to facilitate cross-border access to four categories of data: subscriber data, access data, transactional data and stored content data, directly from the service providers in other jurisdictions. The proposed scenario of cooperation redefines the role that mutual trust plays in cross border evidence-gathering. Therefore, the aim of this research paper is to verify whether the European Union can afford this new model of cooperation in a tentative environment of mutual trust.

Keywords

electronic evidence, mutual trust, European Investigation Order

Introduction[1]

Over the years, the European Union has striven for a functionable instrument that would finally shape the, still non-existent, concept of mutual recognition of evidence

1 The paper has been supported by grant 2016/23/D/HS5/00182 awarded by the National Science Centre, Poland.

in criminal matters and replace the mutual legal assistance regime with a model which is underpinned by mutual trust, based on the principle of mutual recognition. This long-term plan has been gradually slowed down by decreasing faith in mutual trust, originally presumed to exist between the Member States due to their shared commitment to human rights, the rule of law and democracy. In these circumstances, the European Union has introduced its flagship instrument for evidence-gathering, the European Investigation Order[2] (hereafter: EIO), which now plays a leading role in both obtaining and transferring evidence in criminal matters among the Member States. The context in which the EIO has grown, however, has impacted on a shape of this instrument, especially when it comes to its consistency with the principle of mutual recognition. Hence, it foresees a set of provisions which demonstrate mutual distrust, acknowledges possible breaches of fundamental rights and offers withdrawal scenarios in cases of conflicting, domestic standards for evidence-gathering. As it is, the EIO sets the scene for the forthcoming, legal framework governing electronic evidence, which significantly differs, in nature and scope, from the previous, mutual legal assistance and mutual recognition instruments, and also redefines the role of mutual trust.

This research paper analyses the electronic, evidence framework through the lens of mutual trust. The first section presents how the evidence-gathering instruments have evolved over the years as well as the main trust-related challenges. It also explains the need for a specific framework for electronic evidence and the main features that stem from this need. The second section outlines the mutual trust evolution, from overly optimistic, politically presumed full faith and trust to openly distrustful provisions, which, together, have set the scene for an electronic evidence framework. Against this backdrop, the third section measures the level of mutual trust using the EIO provisions and confronted with the specific modalities of the EU proposal. The aim is to verify whether the European Union can afford this new model of cooperation in the tentative, mutual trust environment.

1. The EU evidence-gathering environment

In the pre-mutual, recognition era, cooperation in evidentiary matters was mainly (but not only)[3] governed by the EU 2000 MLA Convention.[4] The Convention introduced a set of substantially interesting and important novelties, such as the *forum regit actum* principle

2 Directive 2014/41/EU regarding the European Investigation Order in criminal matters [2014] OJ L 130/1.

3 Other relevant levels of cooperation were the Council of Europe, the Benelux Economic Union, the Nordic Union, and within the EU, the Schengen *acquis* and customs administration level.

4 Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union [2000] OJ C 197/3.

(hereafter: FRA),[5] spontaneous information exchange at the judicial level of cooperation and direct transmission of requests for mutual assistance. This new framework of mutual assistance, created by the EU 2000 MLA Convention and supplemented by the Protocol of 2001, has been criticised for being far from complete as well as for showing a certain lack of balance.[6] At the same time, the Convention was not supposed to be the prime framework for EU evidence-gathering since the entire mutual assistance *acquis* (including the novelties and changes brought by the 2000 Convention and the 2001 Protocol) was going to be replaced in the years to come with mutual recognition schemes building on politically presumed full faith and trust between the Member States.[7]

Thus in 2003, the European Union launched its first mutual recognition-based instrument, the freezing order.[8] This order established the rules under which a Member State shall recognise and execute, in its own territory, a freezing order issued by a judicial authority of another Member State in order to secure objects, documents or data which could be produced as evidence in criminal proceedings in the issuing Member State. This instrument was limited in its scope and did not foresee exequatur procedures. It also abandoned a dual criminality check for offences qualified as so-called 'Euro crimes', which was a clear demonstration of a certain level of mutual trust between the Member States. The next step towards a mutual recognition system for evidence, which was closely linked to the freezing order, was the European Evidence Warrant[9] (launched in 2008). This warrant was designed to obtain and transmit objects, documents and data from other Member States for use in criminal proceedings in the issuing Member State. This instrument contained modalities that are typical for mutual recognition, such as the departure from a dual criminality check, if no house search is required, and for 'Euro crimes'. It is worth noting that the European Evidence Warrant was, to some extent, used to test the political feasibility of introducing more trust-oriented measures and to further limit double criminality. The Member States, however, were reluctant in this regard and the provisions concerning the mutual availability of measures were only partially incorporated.[10]

---

5 According to this principle, the Member State receiving a mutual legal assistance request must in principle comply with the formalities and procedures expressly indicated by the requesting Member State unless they cause incompatibilities with the fundamental principles of the law of the executing Member State.

6 Gert Vermeulen, 'A EU conventions enhancing and updating traditional mechanisms for judicial cooperation in criminal matters' (2006) 77 Revue internationale de droit pénal 79-95.

7 Ibid.

8 Council Framework Decision 2003/577/JHA on the execution in the European Union of orders freezing property or evidence [2003] OJ L 196/45.

9 Council Framework Decision 2008/978/JHA on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters [2008] OJ L 350/72.

10 Charles Williams, 'The European Evidence Warrant: the Proposal of the European Commission' (2005) ERA Forum: Special Issue on European Evidence 25; Martyna Kusak, *Mutual admissibility of evidence in criminal matter: a study of telephone tapping and house search* (Maklu 2016) 80-82.

Although the European Evidence Warrant did not cover the obtainment of other types of evidence, the Commission considered it to be the first step towards replacing the existing regime of mutual assistance within the European Union by a single EU body of law based on mutual recognition and subject to minimum safeguards.[11] This plan, however, failed. The reason for this was that both of the mutual recognition instruments only covered existing evidence. This proved to be insufficient in the field of EU, cross-border evidence gathering, which, at the time still, mostly, relied on the mutual legal assistance provisions.

A new solution was sought and the European Union then deviated from a step-by-step approach (that inevitably led to fragmentation of the evidence-gathering regimes) to a comprehensive system, based on the principle of mutual recognition (MR), for the obtainment of evidence in cases with a cross-border dimension. This new system was launched in 2014 (with a transposition date of 2017) with a single instrument,[12] the European Investigation Order (hereafter: EIO), which governs both the collection of evidence (including real-time measures) and the obtainment of evidence that is already in the possession of the executing authority. The main reason that it was impossible, for almost a decade, to reach final agreement on the EIO, was the lack of political consensus and the reluctance of Member States to introduce the instrument, unsupported by measures to enhance mutual trust in the evidentiary context. Indeed, over the 20 years in which a considerable body of MR-based EU legal instruments have been introduced, mutual trust has been questioned and this has also had an impact on negotiations on the EIO. Therefore, the final version of the EIO reflects the decreasing level of mutual trust. This has resulted in a lack of inner coherency and doubtful consistency with the pure, mutual recognition philosophy. Despite ambitious plans,[13] the EIO was ultimately not accompanied by any minimum standards to facilitate the admissibility of evidence gathered by means of this instrument, which has also had an impact on its efficiency.

---

11 Proposal for a Council Framework Decision on the European Evidence Warrant for obtaining objects, documents and data for use in proceedings in criminal matters, Brussels, 14 November 2003, COM(2003) 688 final.

12 It is, however, controversial to call the EIO a single instrument given that its Article 34 and the blurred scope of the term 'corresponding provisions' results in the use of some provisions of the EU 2000 MLA Convention. In addition, relations with Denmark and Ireland are still governed by the freezing order and the above-mentioned Convention.

13 Green paper on obtaining evidence in criminal matters from one Member State to another and securing its Admissibility, Brussels, 11 November 2009, COM(2009) 624 final; Commission, Communication on the mutual recognition of judicial decisions in criminal matters and the strengthening of mutual trust between Member States [2005], COM(2005) 195 final; Commission, An area of freedom, security and justice serving the citizen, Brussels, 10 June 2009, COM (2009) 262 final; Commission, Delivering an area of freedom, security and justice for Europe's citizens. Action Plan Implementing the Stockholm Programme, Brussels, 20 April 2010, COM(2010) 171 final; see also Gert Vermeulen, Wendy De Bondt and Yasmine Van Damme, *EU cross-border gathering and use of evidence in criminal matters. Towards mutual recognition of investigative measures and free movement of evidence?* (Maklu 2010) 113; Gert Vermeulen, *Free gathering and movement of evidence in criminal matters in the EU. Thinking beyond borders, striving for balance, in search of coherence* (Maklu 2011) 44-45.

Shortly after the EIO was introduced, it became evident that, at first glance, a broad scope would not be capable of addressing all fields of evidence gathering in the European Union. Rapid, digital progress has an increasing impact on the way humans live and communicate. This, in turn, affects the way in which criminal investigations are conducted. Consequently, not only cybercrime but a large number of other criminal offences are committed in a way that leaves digital traces that can serve as evidence. In order to effectively investigate and prosecute these offences, law enforcement agencies must have access to the digital data, which is mostly in the possession of service providers that are often located abroad. At an international level, this results in the need to resort to mutual, legal assistance and, at the EU level, to the European Investigation Order. Even the time needed to make use of the EIO procedure is far too protracted as relevant data can be lost in the meantime.[14] Therefore, it became necessary to develop a specific, more streamlined mechanism for the preservation and production procedures for electronic data stored by service providers, as well as to relieve the pressure on the mutual assistance system used in relations with non-EU states.[15] Hence, the European Union, in 2018, launched a Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters[16] (hereafter: Proposal) and a Proposal for a Directive of the European Parliament and of the Council, laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings.[17] The proposed regulation introduces rules to facilitate cross-border access to four categories of data: subscriber data,[18] access data,[19]

14 Stanisław Tosza, 'The European Commission's Proposal on Cross-Border Access to E-Evidence. Overview and Critical Remarks' [2018] (4) EUCRIM <https://doi.org/10.30709/eucrim-2018-021>.

15 Since mutual assistance requests are often addressed to states which are hosts to a large number of service providers but which have no other relation to the case at stake.

16 Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, Brussels, 17 April 2018, COM(2018) 225 final.

17 Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, Strasbourg, 17 April 2018, COM(2018) 226 final.

18 'Subscriber data' means any data pertaining to: (a) the identity of a subscriber or customer such as the provided name, date of birth, postal or geographic address, billing and payment data, telephone, or email; (b) the type of service and its duration including technical data and data identifying related technical measures or interfaces used by or provided to the subscriber or customer, and data related to the validation of the use of service, excluding passwords or other authentication means used in lieu of a password that are provided by a user, or created at the request of a user, Article 2 of the Proposal.

19 'Access data' means 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 user ID. This includes electronic communications metadata as defined in point (g) of Article 4(3) of [Regulation concerning the respect for private life and the protection of personal data in electronic communications], Article 2 of the Proposal.

transactional data[20] (the three categories commonly referred to jointly as 'non-content data') and stored content data.[21] The model adopted in the Proposal brings forward a European legal framework for electronic evidence which imposes an obligation on service providers covered by the scope of the instrument to respond directly to authorities without the involvement of a judicial authority in the Member State of the service provider.[22] The numerous, ongoing consultations will, very likely, have a reshaping effect on the e-evidence proposal, however, it is conceivable that a direct cooperation model will be introduced.[23]

2. UPS AND DOWNS OF MUTUAL TRUST

Back in the early 2000s, the European Union operated under strong, politically presumed mutual trust between the Member States which was grounded, in particular, on their shared commitment to the principles of freedom, democracy and respect for human rights, fundamental freedoms and the rule of law.[24] This assumption was incorporated into the flagship mutual recognition instrument, the European Arrest Warrant.[25] After a few years of functioning with the EAW, the European Union began to gradually

20 'Transactional data' means data related to the provision of a service offered by a service provider that serves to provide context or additional information about such service and is generated or processed by an information system of the service provider, such as the source and destination of a message or another type of interaction, data on the location of the device, date, time, duration, size, route, format, the protocol used and the type of compression, unless such data constitutes access data. This includes electronic communications metadata as defined in point (g) of Article 4(3) of [Regulation concerning the respect for private life and the protection of personal data in electronic communications], Article 2 of the Proposal.

21 'Content data' means any stored data in a digital format, such as text, voice, videos, images and sound other than subscriber, access or transactional data, Article 2 of the Proposal.

22 Recital 9 of the Proposal.

23 Direct contact between the competent authorities and service providers has already been enacted at the Council of Europe level, acknowledging the importance of timely cross-border access to electronic evidence in specific criminal investigations or proceedings in view of the challenges posed by existing procedures for obtaining electronic evidence from service providers in other countries, see Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Explanatory Report [2021] <https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4b> accessed 1 February 2022 point 9.

24 Programme of measures to implement the principle of mutual recognition of decisions in criminal matters [2001] OJ C 12/10.

25 Framework decision on the European arrest warrant and the surrender procedures between Member States [2002] OJ L 190/1 and its Recital 10: The mechanism of the European arrest warrant is based on a high level of confidence between Member States. Its implementation may be suspended only in the event of a serious and persistent breach by one of the Member States of the principles set out in Article 6(1) of the Treaty on European Union, determined by the Council pursuant to Article 7(1) of the said Treaty with the consequences set out in Article 7(2) thereof.

acknowledge the more political, than genuine, foundations of mutual trust[26]. The 2005 Hague Programme[27] talks about 'strengthening' mutual trust by the progressive development of a European judicial culture based on the diversity of the legal systems of the Member States and unity through European law. Communication on the mutual recognition of judicial decisions in criminal matters and the strengthening of mutual trust between Member States [2005] refers to 'reinforcing' mutual trust by legislative measures.[28] The 2010 Stockholm Programme talks of finding new ways to 'increase reliance' on mutual trust,[29] which requires minimum standards and a reinforced understanding of the different legal traditions and methods[30]. Over the years also the CJEU has challenged the shape of mutual trust. In its early judgements of *Advocaten voor de Wereld*[31] and *Melloni*,[32] the Court operated under strong, mutual trust, whereas the newer judgements[33] have brought a significant, fundamental-rights driven[34] change to

26 See the criticism about the absence of an explicit ground for refusal based on human rights violations in: Anne Weyembergh, 'European Added Value Assessment The EU Arrest Warrant ANNEX I Critical Assessment of the Existing European Arrest Warrant Framework Decision' (2014) <https://doi.org/10.2861/44748>; <https://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/510979/IPOL-JOIN_ET(2013)510979(ANN01)_EN.pdf>, accessed 24 May 2022.

27 The Hague Programme: Strengthening Freedom, Security and Justice in The European Union [2005] OJ C 53/1.

28 Commission, Communication on the mutual recognition of judicial decisions in criminal matters and the strengthening of mutual trust between Member States, Brussels, 19 May 2005, COM(2005) 195 final, para 19: 'The first endeavours to apply the MR principle, in particular with the European arrest warrant, revealed a series of difficulties which could to some extent be resolved if the Union were to adopt harmonisation legislation. This can revolve around two axes: ensuring that mutually recognised judgments meet high standards in terms of securing personal rights and also ensuring that the courts giving the judgments really were the best placed to do so. Taking MR a stage further might imply giving further consideration to certain measures to approximate legislation on substantive criminal law'.

29 The Stockholm Programme – An Open And Secure Europe Serving And Protecting Citizens [2010] OJ C 11/1: 1.2.1. '*Mutual trust. Mutual trust* between authorities and services in the different Member States and decision-makers is the basis for efficient cooperation in this area. Ensuring trust and, and mutual understanding between, the different legal systems in the Member States will thus be one of the main challenges for the future'.

30 Commission, Delivering an area of freedom, security and justice for Europe's citizens, (n 13): 'The European judicial area and the proper functioning of the single market are built on the cornerstone principle of mutual recognition. This can only function effectively on the basis of mutual trust among judges, legal professionals, businesses and citizens. Mutual trust requires minimum standards and a reinforced understanding of the different legal traditions and methods. Establishing rights is not enough. Rights and obligations will become a reality only if they are readily accessible to those entitled to them. Individuals need to be empowered to invoke these rights wherever in the Union they happen to be'.

31 Case C-303/05 *Advocaten voor de Wereld VZW,* EU:C:2007:261.

32 Case C-399/11 *Melloni,* EU:C:2013:107.

33 Case C-404/15 *Aranyosi Căldăraru,* EU:C:2016:198; Case C-216/18 *LM,* EU:C:2018:586; Joined Cases C-354/20 and C-412/20 *L and P,* EU:C:2020:1033.

34 Tomasz Ostropolski, 'Współpraca wymiarów sprawiedliwości w sprawach karnych' in Jan Barcz (ed), *Współpraca sądowa w sprawach cywilnych, karnych i współpraca policyjna. System Prawa Unii Europejskiej,* Vol. 8 (C.H. Beck 2021) 296-305.

this approach. This gives rise to a fundamental question: Has there ever been a sufficient, genuine and unambiguous foundations of 'mutual trust' basis in place?

3. Evidence gathering and mutual trust: the lessons from the EIO

The EIO, which was designed to exist in the fluctuating mutual trust environment, raises a number of concerns with regard to the lawfulness of the evidence obtained using this instrument and the level of protection of the fundamental rights of the persons involved in cross-border investigative measures.[35] In opposition to this approach, the European Union launched its proposal on electronic evidence, which is a door opener to free movement of electronic data across the Member States. It has to be stressed that the e-evidence Proposal is not a typical mutual recognition instrument since it ensures the mutual recognition of those judicial decisions in which a judicial authority in the issuing jurisdiction directly addresses and imposes obligations on a service provider from another jurisdiction (including those beyond the EU) without the prior intervention of a judicial authority in that other Member State.[36] Both the European Production or Preservation Order can lead to the intervention of a judicial authority of the executing State only if there is non-compliance, in which case enforcement will be required and the competent authority in the country in which the representative is located will intervene (in the role of an 'enforcing authority'). Nevertheless, as a principle, an authority in the country where the addressee of the order is located will not have to be directly involved in serving and executing the order. The e-Proposal has thus switched mutual recognition from the judicial level to the level of judicial–private data controllers.[37] This means the role of mutual trust has also changed: whereas it has traditionally been looked upon as two-directional trust divided between the executing (trusting the issuing) and issuing (trusting the executing) Member States,[38] now it seems to lose this significance.

35 Balázs Garamvölgyi, Katalin Ligeti, Anna Ondrejová, Margarete von Galen, 'Admissibility of Evidence in Criminal Proceedings in the EU' [2020] (3) EUCRIM <https://doi.org/10.30709/eucrim-2020-016>; Hanna Kuczyńska, 'Admissibility of Evidence Obtained as a Result of Issuing an European Investigation Order in a Polish Criminal Trial' (2021) 46 Review of European and Comparative Law 67 <https://doi.org/10.31743/recl.11815>.

36 Angel Tinoco-Pastrana, 'The Proposal on Electronic Evidence in the European Union' [2020] (1) EUCRIM <https://doi.org/10.30709/eucrim-2020-004>.

37 Marcin Rojszczak, 'e-Evidence Cooperation in Criminal Matters from an EU Perspective' (2022) Modern Law Review <https://doi.org/10.1111/1468-2230.12749>.

38 See elaborately Gert Vermeulen 'The EU's mutual trust and recognition bubble – Challenging the legitimacy of EU criminal policy and judicial cooperation in criminal matters' in Klaus Tiedemann, Urlich Sieber, Helmut Datzger, Christoph Burchard and Dominik Brodowski (eds), *Die Verfassung moderner Strafrechtspflege* (Nomos 2016) 181-210.

3.1. Fundamental rights protection

The proposed model for gathering e-evidence puts a lot of pressure on the issuing State and authority since the domestic law of this country will fully govern the process involved in accessing electronic data *via* a foreign service provider. The lack of judicial recognition in the executing Member State raises doubts about the level of protection of the fundamental rights of the data subjects, even though a direct channel of cooperation with service providers is necessary in view of the growing need for timely cross-border access to electronic evidence. The EIO is a good example here since it expressly acknowledges that breaches of fundamental rights may occur. Article 11(1)(f) introduces fundamental, rights-based grounds for refusal which free the executing State from executing the order if there are substantial grounds to believe that the execution of the investigative measure indicated in the EIO would be incompatible with the executing State's obligations in accordance with Article 6 TEU and the Charter.

As controversial as it is,[39] Article 11(1)(f) of the EIO Directive, both anticipates a fundamental rights breach scenario and provides the executing authority grounds for refusal. However, the Proposal puts a service provider (namely, an actor outside the criminal justice system) in charge. If the provider considers that the order manifestly violates the Charter of Fundamental Rights, it shall turn to the competent enforcement authority in the Member State concerned. In such cases, the competent enforcement authority may seek clarification from the issuing authority of the European Production Order either directly, via Eurojust or the European Judicial Network (Article 9(5)). This seems to impose a lot of responsibility on service providers who would actually be on the front line to detect 'manifest violations' that may lead to fundamental rights violations.

There is no convincing reason to believe that the gathering of electronic evidence will not provoke such breaches, especially since the EIO simply accepted the fact that fundamental rights-based concerns are inevitable. A closer look at the data which may be sought, which consists of both content and non-content data, will help to illustrate the potential scale of abuses. It is true that obtaining basic, subscriber information just for identification purposes (such as an account holder's name and address) is generally less invasive than obtaining transactional or content data. However, it is also true that non-content data, taken as a whole, is liable to cause very precise conclusions to be drawn concerning the private lives of the persons whose data was retained, thereby establishing a profile of the individuals concerned.[40] Leaving the power to access content data stored abroad with the issuing authorities also seems controversial as the domestic preconditions for such measures vary considerably.[41] Is also should be noted that at the

39 Due to its clear inconsistence with the mutual trust concept.

40 Joined Cases C203/15 and C698/15 *Tele2 Sverige* AB, EU:C:2016:970, para 99.

41 Martyna Kusak, 'Mutual admissibility of electronic evidence in the EU. A study of subscriber, access, transactional and content data stored by service providers', forthcoming.

Council of Europe level, the Second Protocol to the Budapest Convention[42] limited the possibility of directly contacting service providers to obtain subscriber data. There is no convincing reason to believe that the European Union operates under a much higher level of trust, which would justify the scope of the data that can be sought using the e-evidence Proposal. Article 1(1) of the Proposal, the Directive 2016/680 on personal data protection[43] and the Charter for Fundamental Rights will not be of much assistance here. A generic, fundamental rights foundation has already proven to be insufficient for enhancing mutual trust in criminal matters.[44] Additionally, data protection is not capable of accommodating all specific, evidence-oriented issues. Thus, it is simply naive to fully rely on the assumed commitment of Member States (in this case the issuing State) to respect fundamental rights.

A solution, which would eradicate these dilemmas, is to introduce common, EU minimum standards for stored subscriber, access, transactional and content data based on Article 82(2) TFEU.[45] Although adequate data protection is guaranteed by Directive 2016/680, which would also act as a default standard for the application of the e-evidence Proposal, the Member States still lack common, transparent terms with regard to the lawfulness of the way electronic evidence is gathered as well as the rules enhancing the procedural rights of the data subjects. Such standards would also play an important trust-building function as they would have an effect between all the agents involved in electronic evidence gathering (judicial authorities, data subjects, service providers), which would facilitate the overall application of the e-evidence framework.

3.2. Proportionality

As with the EIO, the Proposal relies on a self-proportionality assessment by the issuing authority. Again, it seems to be overly optimistic to blindly believe that the domestic preconditions for accessing data will adequately ensure a comparable level of proportionality. The comparative data actually suggests otherwise, in particular with regard to accessing stored content data which significantly differs across the EU Member States.[46] Whereas the EIO counterbalances this proportionality self-assessment with the distrust-based recourse to a different type of investigative measure (Article 10 EIO), the Proposal offers no solution other than for the service provider to resort to the executing State authority.

42 Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence [2021] CM(2021)57 final.

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

44 Vermeulen (n 38) 201-208.

45 This article opens up a possibility to adopt minimum rules facilitating, inter alia mutual admissibility of evidence in criminal matters.

46 Kusak (n 41).

This issue, moreover, could be addressed by means of minimum standards based on Article 82(2) TFEU, which would introduce common preconditions delineating, *inter alia*, proportionality features.

3.3. Speciality

The specialty principle is aimed at the cross-border collection and use of information and evidence and plays a key role in international cooperation in criminal matters, including in the context of mutual legal assistance. Even though it was introduced in the late 1980s, attention on informational or evidential specialty seems to be non-existent in times of post MR-based, mutual legal assistance instruments. The EIO also lacks any provisions or leadership on the *use* limitation for information and evidence gathered with this instrument, which causes a lot of practical difficulties.[47] Research on this issue has revealed that only a more detailed, generic specialty rule and data ownership principle have the potential to promote the free movement of information and evidence whilst equally enhancing the procedural rights positions of persons.[48]

This lesson from the EIO, however, has clearly not been learnt. In addition, the Proposal refrains from delineating for which purposes transferred personal data can be used by the receiving competent authority. In this context, the 'use limitation rules' seem to be of even more importance, given the scope and sensitivity of the data that may be sought.[49] Therefore, the data protection purpose-limitation principle should be promoted to act as a use limitation for personal data gathered under the Proposal, although the two principles do not fully equate with each other either conceptually or functionally.[50]

3.4. Lack of measures enhancing admissibility of evidence

Since the 1999 Tampere conclusions, the European Union has been striving for a model implementing *per se* admissibility of evidence in criminal matters. Since all the initial plans and ambitions failed, the EIO still relies on the *forum regit actum* principle,

47 European Judicial Network (EJN), Extract from the Conclusions of the 49th Plenary meeting of EJN <https://www.ejnforum.eu/cp/registry-files/3373/ST-15210-2017-INIT-EN-COR-1.pdf> 9 accessed 1 February 2022; see also Julio Barbosa e Silva 'The speciality rule in cross-border evidence gathering and in the European Investigation Order – let's clear the air' (2019) 19 ERA Forum 485-504.

48 Gert Vermeulen, Martyna Kusak, 'Unblurring the Fuzzy Line Between Specialty and Data Protection in EU Mutual Legal Assistance after the European Investigation Order', forthcoming.

49 See also the interesting considerations of Gert Vermeulen as to allowing the consent of the data subject as a basis for further use, drawn in the context of the Second Protocol to Budapest Convention, Inclusion of data protection safeguards relating to law enforcement trans-border access to data in the Second Additional Protocol to the Budapest Convention on Cybercrime (ETS 185), Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data, T-PD(2019)3, p. 5.

50 Vermeulen and Kusak (n 48).

which has not been complemented with any rules facilitating admissibility of evidence gathered by use of this instrument. This may lead to situations in which, due to the lack of transparent EU rules, operating under domestic approaches will raise admissibility concerns, lower the procedural guarantees of the persons involved in the measures and render the entire cooperation pointless.

Seemingly, gathering data directly from the service provider does not raise many concerns about the admissibility of evidence. The issuing authority will not be reliant on the procedural rules of the executing State, and the latter will not be involved whatsoever, leaving no room for questioning incompatibilities on access to data. Depending solely on the issuing State's rules may indeed be functional if evidence is to be used solely for the purposes of the ongoing proceedings in that State. It could, however, still be questioned if the data is already in the possession of the criminal justice authorities and is to be transferred to another EU Member State. In such a context, the State seeking the data (using the EIO) will be confronted about the way in which it was obtained by the authority from another EU State, with no opportunities to enhance its admissibility (FRA is clearly helpless here). From this point of view, the EIO and the Proposal are consistent in the fact that no efforts have been made to ensure the mutual admissibility of evidence. This issue can only be accommodated by the trust-building measures, which would reduce the disproportions between the EU Member States, namely the minimum standards based on Article 82(2) TFEU.

3.5. Legal remedies

It is safe to say that mutual trust could be significantly upgraded if the data subject is given effective procedural remedies against the evidentiary measure.[51] Even though the EIO ensures legal remedies equivalent to those available in a similar domestic case (Article 14), it has not made any efforts to ensure that such remedies actually exist. Hence, this provision becomes superfluous in cases in which domestic law does not provide such a remedy or if its execution is not feasible in certain stages of the procedure.

On the contrary, the Proposal introduces the rule that for suspects and accused persons, the right to an effective remedy should be exercised during the criminal proceedings. This may affect the admissibility or, as the case may be, the weight in the proceedings of the evidence obtained by such means. In addition, suspects and accused persons benefit from all procedural guarantees applicable to them, such as the right to information. Other persons, who are not suspects or accused persons, should also have the right to an effective remedy (Recital 56). This change of approach, which finally shapes the so-far patchwork landscape of rules on legal remedies and also serves a trust-building function, should be fully supported.

51 *Rotaru v Romania* App no 28341/95 (ECtHR, 4 May 2000).

CONCLUSIONS

The EIO's specific provisions clearly confirm the low level of mutual trust between Member States in the evidence-gathering context, which is supposed to be balanced by a set of provisions left to the executing authority (*inter alia* recourse to a different type of investigative measure grounds for refusal) and primarily by the FRA principle for the issuing authority. Without introducing any measures towards enhancing such trust, the EU has proposed a model for electronic evidence, which almost entirely relies on the issuing authority and the law of the issuing Member State, redefining the role that mutual trust plays in the mutual recognition context. In this new scenario, there is neither an executive authority entrusted with the way in which the measure was granted in the issuing State, nor the issuing State entrusted with the manner in which the measure was undertaken abroad. Cooperation is conducted directly between the issuing State and service provider unless the former refuses to cooperate or questions the proportionality of the measure. This constellation leads to the impression that, contrary to the EIO, this model can actually work, notwithstanding the insufficient level of mutual trust. However, as this paper reveals, the trust gaps will have a significant, negative impact on various agents and aspects of criminal justice, including the fundamental rights of data subjects, the application of the rule of speciality or mutual admissibility of evidence. The e-evidence Proposal has to be accompanied by modalities which enhance mutual trust across this context, which would also expand the indirect protectionist functions of Directive 2016/680 on personal data protection. This can be achieved by means of introducing minimum standards based on Article 82(2) TFEU which contain transparent terms related to the lawfulness of the way in which electronic evidence is gathered as well as rules enhancing the procedural rights of the data subjects.

BIBLIOGRAPHY

Legal acts

Convention established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union [2000] OJ C 197/3

Framework decision on the European arrest warrant and the surrender procedures between Member States [2002] OJ L 190/1

Council Framework Decision 2003/577/JHA on the execution in the European Union of orders freezing property or evidence [2003] OJ L 196/45

Council Framework Decision 2008/978/JHA on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters [2008] OJ L 350/72

Directive 2014/41/EU regarding the European Investigation Order in criminal matters [2014] OJ L 130/1

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

Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence [2021] CM(2021)57 final

Case law

CJEU

Case C-303/05 *Advocaten voor de Wereld VZW*, EU:C:2007:261

Case C-399/11 *Melloni,* EU:C:2013:107

Case C-404/15 *Aranyosi Căldăraru,* EU:C:2016:198

Joined Cases C203/15 and C698/15 *Tele2 Sverige AB*, EU:C:2016:970

Case C-216/18 *LM,* EU:C:2018:586

Joined Cases C-354/20 and C-412/20 *L and P,* EU:C:2020:1033

ECtHR

Rotaru v Romania App no 28341/95 (ECtHR, 4 May 2000)

Official documents

Programme of measures to implement the principle of mutual recognition of decisions in criminal matters [2001] OJ C 12/10

Proposal for a Council Framework Decision on the European Evidence Warrant for obtaining objects, documents and data for use in proceedings in criminal matters, Brussels, 14 November 2003, COM(2003) 688 final

Commission, Communication on the mutual recognition of judicial decisions in criminal matters and the strengthening of mutual trust between Member States, Brussels, 19 May 2005, COM(2005) 195 final

The Hague Programme: Strengthening Freedom, Security and Justice in The European Union [2005] OJ C 53/1

Commission, An area of freedom, security and justice serving the citizen, Brussels, 10 June 2009, COM (2009) 262 final

Green paper on obtaining evidence in criminal matters from one Member State to another and securing its Admissibility, Brussels, 11 November 2009, COM(2009) 624 final

The Stockholm Programme – An Open And Secure Europe Serving And Protecting Citizens [2010] OJ C 11/1

Commission, Delivering an area of freedom, security and justice for Europe's citizens. Action Plan Implementing the Stockholm Programme, Brussels, 20 April 2010, COM(2010) 171 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, Brussels, 17 April 2018, COM(2018) 225 final

Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, Strasbourg, 17 April 2018, COM(2018) 226 final

European Judicial Network (EJN), Extract from the Conclusions of the 49th Plenary meeting of EJN <https://www.ejnforum.eu/cp/registry-files/3373/ST-15210-2017-INIT-EN-COR-1.pdf> accessed 1 February 2022

Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Explanatory Report [2021] <https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4b> accessed 1 February 2022

Scientific publications

Barbosa e Silva J, 'The speciality rule in cross-border evidence gathering and in the European Investigation Order – let's clear the air' (2019) 19 ERA Forum

Garamvölgyi B, Ligeti K, Ondrejová A, Galen von M, 'Admissibility of Evidence in Criminal Proceedings in the EU' [2020] (3) EUCRIM <https://doi.org/10.30709/eucrim-2020-016>

Kuczyńska H, 'Admissibility of Evidence Obtained as a Result of Issuing an European Investigation Order in a Polish Criminal Trial' (2021) 46 Review of European and Comparative Law <https://doi.org/10.31743/recl.11815>

Kusak M, 'Mutual Admissibility of Electronic Evidence in the EU. A Study of Subscriber, Access, Transactional and Content Data Stored by Service Providers' forthcoming

Kusak M, *Mutual Admissibility of Evidence in Criminal Matter: A Study of Telephone Tapping and House Search* (IRCP Research Series, Vol. 53, Maklu 2016)

Ostropolski T 'Współpraca wymiarów sprawiedliwości w sprawach karnych' in J Barcz (ed), *System Prawa Unii Europejskiej. Współpraca sądowa w sprawach cywilnych, karnych i współpraca policyjna,* Vol. 8 (C.H. Beck 2021)

Rojszczak M, 'e-Evidence Cooperation in Criminal Matters from an EU Perspective' (2022) Modern Law Review <https://doi.org/10.1111/1468-2230.12749>

Tinoco-Pastrana A, 'The Proposal on Electronic Evidence in the European Union' [2020] (1) EUCRIM <https://doi.org/10.30709/eucrim-2020-004>

Tosza S, 'The European Commission's Proposal on Cross-Border Access to E-Evidence. Overview and Critical Remarks' [2018] (4) EUCRIM <https://doi.org/10.30709/eucrim-2018-021>

Vermeulen G, 'A EU Conventions Enhancing and Updating Traditional Mechanisms for Judicial Cooperation in Criminal Matters' (2006) 77 Revue internationale de droit pénal

Vermeulen G, *Free Gathering and Movement of Evidence in Criminal Matters in the EU. Thinking Beyond Borders, Striving for Balance, in Search of Coherence* (Maklu 2011)

Vermeulen G, 'The EU's Mutual Trust and Recognition Bubble – Challenging the Legitimacy of EU Criminal Policy & Judicial Cooperation in Criminal Matters' in K Tiedemann, U Sieber, H Datzger, Ch Burchard, D Brodowski (eds), *Die Verfassung moderner Strafrechtspflege* (Nomos 2016)

Vermeulen G, Bondt De W, Damme Van Y, *EU Cross-Border Gathering and Use of Evidence in Criminal Matters. Towards Mutual Recognition of Investigative Measures and Free Movement of Evidence?* (Maklu 2010)

Vermeulen G, Kusak M, 'Unblurring the Fuzzy Line Between Specialty and Data Protection in EU Mutual Legal Assistance after the European Investigation Order' forthcoming

Weyembergh A, 'European Added Value Assessment The EU Arrest Warrant ANNEX I Critical Assessment of the Existing European Arrest Warrant Framework Decision' (2014) <https://doi.org/10.2861/44748>

Williams C, 'The European Evidence Warrant: the Proposal of the European Commission' (2005) 25 ERA Forum: Special Issue on European Evidence

Information about the Author

Martyna Kusak is an Adjunct Professor at the Chair of Criminal Procedure, Adam Mickiewicz University in Poznań (Poland) and a postdoc collaborator at the Institute for International Research on Criminal Policy, Ghent University (Belgium). Ms. Kusak's research focuses on European cooperation in criminal matters, data protection, big data and artificial intelligence in criminal matters. ORCID 0000-0002-7596-9022. E-mail: m.kusak@amu.edu.pl.