'Catch me if you can!' - Evaluation of the European Union E-Evidence Package Proposal (case study of Meta Inc.)

Themis 2022

Semifinal A - *EU and European Criminal Procedure*

Team:

Wojciech Antosiak

Jan Sukiennik

Karolina Sztachańska

Tutor:

Barbara Augustyniak

Abstract

Nowadays, crimes are increasingly committed online by using information systems and electronic communication networks. Such acts leave fragile and volatile digital traces. Obtaining them effectively is a huge challenge for current criminal proceedings. Since cyberspace knows no borders, collecting digital evidence requires mutual legal cooperation, not only between legal authorities but also with various service providers. Attempts to regulate that cooperation were made by the EU decision-making bodies and eventually materialized in the proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters.

In this paper we take a closer look at that project, ranging from brief history of mutual legal assistance between the EU and third parties, to the Regulation itself, its content, aims, as well as different points of view of particular institutions which worked on that legal act. Finally, we present our critical assessment of the Regulation including its potential effectiveness and sufficiency for current needs of criminal proceedings.

Keywords: mutual legal assistance, e-evidence package, European Production Order, European Preservation Order, obtaining digital evidence, criminal proceedings

I. Introduction

It is hard to imagine today a world without technology, especially the Internet. For the last few decades, the digital world has evolved, and the creativity of criminal offenders did, too. We all know that the criminals are developing effective tools to make evidence hard to discover and gather by the police and legal authorities. Therefore, tracing a particular perpetrator is getting more and more difficult and requires unconventional reactions and solutions. However, the high flexibility and borderless nature of digital tools as well as necessity of transparency of actions used by legal authorities put investigations in kind of slow motion. In the meantime, while investigation is pending, digital data with its fragileness is constantly changing and, moreover, disappearing. On top of that, providers, especially giants like Meta Inc., are reluctant to cooperate, and do not want to voluntarily share their data. Then, how to catch the uncatchable and to put it in the box called 'the digital evidence'? The European legal environment actively deals with that problem. So far, it affected the creation of an array of legal acts, called the 'E-Evidence Package'. However, is it going to be enough to protect digital space and improve efficiency of criminal proceedings? In this paper we take a look at the evolution of mutual legal assistance instruments throughout the years in the context of cross-border gathering of e-evidence. Then, we analyze the so-called 'E-Evidence Package', the newest tool of the European Union used to bring the fight against cybercrime into the 21st century. Finally, we evaluate the usefulness of that tool.

II. European cooperation in the field of e-evidence - an historical review

The process of shaping European cooperation on obtaining cross-border electronic evidence is long-lasting and open-ended. The date of 20 March 1959 can be regarded as a starting point of that process. Just then, the European Convention on Mutual Assistance in Criminal Matters (ECMA)[1] was opened for signatures. The truth is that that treaty did not contain any specific rules on e-evidence, but it provided a framework of judicial international cooperation in criminal matters. In particular, the ECMA provisions set out the basic requirements for requests,[2] grounds for refusals[3] and the principle of communication between central authorities of cooperating states.[4] In accordance with the article 15, requesting directly to judicial authority was admissible only in case of urgency. It is important that there was no

[1] The European Convention on Mutual Assistance in Criminal Matters 1959, ETS 030.
[2] Ibid., art. 14.
[3] Ibid., art. 2.
[4] Ibid., art. 15.

time limit for execution of requests, but requesting countries were able to ask other countries to state the date until which the request should have been processed.

The ECMA still needed some improvements and therefore the Additional Protocol to the ECMA (ECMA-1P)[5] was opened for signatures on 17 March 1978. However, this supplementation did not impact on gathering cross-border electronic evidence except the fact that one of reasons for the refusal has been removed.[6]

Another important date was 19 June 1990, when Convention implementing the Schengen Agreement of 14 June 1985 (CISA)[7] was signed. In contrast to above-mentioned regulations, that document was not the initiative of the Council of Europe, but it was a manifestation of cooperation within European Communities. On the other hand its chapters connected to mutual assistance in criminal matters served to supplement the ECMA.[8] The CISA is worthy of mentioning here, because on the grounds of its provisions the principle of communication between central authorities has been replaced by the principle of direct communication between judicial authorities of cooperating states.[9] However, parties kept the possibility of requests being sent and returned between Ministries of Justice or through national central bureaus of the Interpol.[10] The CISA still did not contain specific rules of obtaining e-evidence and any time limits for realization of requests.

On 29 May 2000 the Council of the European Union established the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (EUCMA).[11] It served to supplement the ECMA, the ECMA-1P and the CISA. The principle of direct communication between judicial authorities was confirmed under its provisions. Only the United Kingdom and Ireland gained the right to declare that requests had to be sent via its central authority,[12] but other states saved the possibility to cooperate with central authorities in specific cases and got the right to apply the principle of reciprocity in relation to potential Irish and British declarations.[13] It is significant, that in emergencies, parties were authorized to send requests via Interpol or other body competent under rules adopted pursuant

[5] Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters 1978, ETS 099.
[6] Ibid., art. 1.
[7] Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders 1990, OJ 2000 L 239/19.
[8] Ibid., Art. 48.
[9] Ibid., Art. 53(1).
[10] Ibid., Art. 53(2).
[11] OJ 2000 C 197/3.
[12] Ibid., Art. 6(2); Art. 6(3).
[13] The admissibility of the communication between two central authorities or between judicial authority and central authority. Ibid., Art. Article 6(2).

to the Treaty on European Union.[14] On the grounds of EUCMA, the requested country was obliged to comply with the formalities and procedures specified by the requesting country.[15] Similar to previous conventions and protocols, the EUCMA did not contain specific rules connected to gathering e-evidence and time limits for execution of request, except some provisions related to interception of telecommunications.[16] The EUCMA became effective on 23 August 2005. On 16 October 2001 the EUCMA was supplemented by protocol,[17] which added some provision about requests for information on bank accounts to it.

The November of the year 2001 was particularly important for the described process. On 8 November, the Second Additional Protocol to the ECMA (ECMA-2P)[18] was opened. There was no doubt that the ECMA, which was nearly 50 years old, needed some improvements. The principle of communication between central authorities was limited and parties got the possibility to communicate with each other via judicial authorities.[19] However, each participant was authorized to reserve the right to make the execution of requests dependent on one or more conditions stated in article 15 (8) of the supplemented ECMA.

The protocol did not introduce any other changes in case of gathering e-evidence. However, this subject was well covered by Council of Europe's Convention on Cybercrime,[20] which was opened for signatures on 23 November 2001, only 15 days after the ECMA-2P. That treaty was known '*to constitute the first and most significant multilateral binding instrument to regulate cybercrime*'.[21]That act contained definitions of terms such as 'computer system', 'computer data', 'service provider' and 'traffic data'.[22] Apart from provisions related to substantive criminal law,[23] the CCC embraced some procedural provisions, including measures concerning both domestic and cross-border access to evidence in electronic form. According to Article 25, all the CCC's Parties were obliged to afford one another mutual assistance to the widest extent possible for the purpose of collection of electronic evidence. Cooperating CCC's Parties, which were not bound by mutual assistance treaties or bilateral

[14] Ibid., Art. 6(4).
[15] Ibid., Art. 4(1).
[16] Ibid., Title III, in particular Art. 20 (4).
[17] Protocol established by the Council in accordance with Article 34 of the Treaty on European Union to the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ 2001 C 326/2.
[18] Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters 2001, ETS 182.
[19] Ibid., Art. 4.
[20] Convention on Cybercrime 2001, ETS 185.
[21] Blažič and Klobučar, 'Removing the barriers in cross-border crime investigation by gathering e-evidence in an interconnected society', 29 *Information & Communications Technology Law* (2020) 66, at 68.
[22] Convention on Cybercrime, *supra* note 20, Art. 1.
[23] Ibid., Art. 2 – 13.

agreements between them, were obliged to respect rules expressed in Articles 28 and 29, which were more or less the same as the ECMA's and the 20 EUCMA's rules. At the same time, all parties got the possibility of requesting that another state preserves the data stored in the computer system, located within the territory of another country. By that mechanism, electronic evidence could be protected from destruction, deletion and modification for a period of at least 60 days,[24] until the execution of a traditional MLA request was stopped. Moreover, all parties had right of direct access to data stored in other country if the data was publicly available[25] or if the data was accessed or received through a computer system in requesting state's territory if the Party, where evidence was stored, obtained the lawful and voluntary consent of the person who had the lawful authority to disclose the data to the requesting State through that computer system.[26] To increase the efficiency of the cross-border cooperation in the area of electronic evidence, all Parties were obliged to designate points of contact available on a twenty-four hour, seven-day-a week basis.[27]

Next important steps in the process were made on 22 July 2003, when the Council Framework Decision 2003/577/JHA (CFD577)[28] was established, and on 18 December 2008, when Council Framework Decision 2008/978/JHA (CFD978)[29] was signed. Provisions of the first document were restricted only to the freezing phase and they served to prevent the destruction, transformation, moving, transfer or disposal of evidence. The European Evidence Warrant, which was a judicial decision issued by a competent authority of a Member State with a view to obtaining objects, documents and data from another Member State, was introduced by the second one. In accordance with article 4 (2e) use of this instrument was unacceptable in the case of obtaining communications data retained by providers of a publicly available electronic communications service or a public communications network. Both documents did not have crucial influence on gathering e-evidence, but they became the basis for the European Investigative Order (EIO), which should be pointed as the milestone in the process.

That instrument was established by Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in Criminal

[24] Ibid., Art. 29 (7).
[25] Ibid., Art. 32 (a).
[26] Ibid., Art. 32 (b).
[27] Ibid., Art. 35.
[28] Council Framework Decision 2003/577/JHA on the execution in the European Union of orders freezing property or evidence was established, OJ 2003 L 196/45.
[29] 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, OJ 2008 L 350/72. This document was transposed only by six countries (Spain, Croatia, Netherlands, Romania, Slovenia and Finland).

Matters (EIOD).[30] An EIO was based on two principles: the principle of mutual recognition[31] and the principle of proportionality.[32] Moreover, it served to simplify the process of obtaining cross-border evidence particularly by providing standardization and to replace previous tools. The EIO was introduced as a judicial decision issued or validated by a judicial authority[33] of a Member State to have one or several specific investigative measures carried out in another Member State to obtain evidence in accordance with the EIOD.[34] It was significant that the executive State could refuse recognition or execution of an issued EIO only in exceptional cases.[35] The execution of an EIO normally should have been carried out within a maximum of 150 days of receipt of the EIO,[36] but it was important to underline that the executive authority could have been asked to do it on a specific date. The EIOD did not contain specific e-evidence gathering procedure except for proceedings of interception of telecommunications.[37] On the other hand, in accordance with article 10 (2e) the identification of persons holding a subscription of a specified phone number or IP address was pointed out as one of the measures, which could not be substituted by others.[38] The EIOD became effective on 21 May 2014.

The last step, which should be mentioned here, was made on 17 November 2021, when the Second Additional Protocol to the CCC (CCC-2P)[39] was adopted by the Committee of Ministers of the Council of Europe. In accordance to its provisions, all CCC-2P Parties shall adopt such legislative and other measures as may be necessary to empower its competent authorities in particular to issue a direct request to entities providing domain name registration services in the territory of another Party[40] or service providers in the territory of another Party[41] for information for identifying or contacting the registrant of a domain name or for stored subscriber information respectively. Under CCC-2P provisions, data providers shall respond within 30 days of receipt of the order or the stipulated timeframe.[42] If a timeframe is

[30] Directive 2014/41/EU, OJ 2014 L 130/1.
[31] Ibid., Recital 19; Art. 1 (2).
[32] Ibid., Art. 6; Art. 10; and 10 (3); Recital 11.
[33] The EIO can be issued by a judge, a court, an investigating judge or a public prosecutor. It can also be issued by another competent authority with power granted by national law of an EU Member, but in this case the EIO has to be validated by one of the above-mentioned authorities.
[34] Directive 2014/41/EU, *supra* note 32, Art. 1(1).
[35] Ibid., Art.11 (1); Art. 30 (5).
[36] Ibid. Art. 12 (3 – 5).
[37] Ibid., Art. 30; Art. 31.
[38] In principle, executing authorities have the right to recourse to an investigative measure other than that provided for in the EIO in the situation described in article 10 (1) EIOD.
[39] Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence 2022.
[40] Ibid., Art. 6.
[41] Ibid., Art. 7.
[42] Ibid., Art. 7 (7).

exceeded, the requesting authority shall have an opportunity to ask the competent authority of the data provider's state for additional legal assistance.[43] A minimum framework on request orders' content is also established by provisions of the CCC-2P. That document will be presented for signatures in Strasbourg on 12 May 2022.[44]

III. The current situation in obtaining e-evidence

Nowadays, the majority of above referenced acts are still binding.[45] There is no doubt that the EIO has become the basic instrument to gather and transfer electronic evidence between European Union Member States except for Ireland and Denmark. It means that requests issued to Ireland are generally based on the ECMA,[46] its protocols[47] and the EUCMA.[48] Moreover, both in the case of the ECMA and the EUCMA, Ireland exercised its right to declare that all requests on mutual assistance, addressed to this state, shall be sent to its central authority.[49] At the same time, it is important to mention that Ireland hasn't ratified the CCC, which binds another 66 countries, including the US. Apart from CCC, rules of cooperation in criminal matters between the US and EU Countries are regulated by bilateral agreements and the Agreement on mutual legal assistance between the European Union and the US, published in the Official Journal on 19 March 2003. However, on 23 March 2018 the President of the US signed the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), which allows the US President to enter 'executive agreements' with foreign countries. These agreements are founded on the principle of mutual access to data stored outside each party territory. With this instrument EU Countries will gain an opportunity to speed up gaining access to electronic evidence stored by a data provider located in the US by omitting a standard court procedure.[50] Currently, the EC, acting on behalf of the European Union,[51] is conducting the negotiations for this kind of agreement between the US and EU.

---

[43] Ibid., Art. 7 (7); Art. 8.
[44] Council of Europe Portal, *New Treaties* (2022), available at https://www.coe.int/en/web/conventions/new-treaties.
[45] Only Council Framework Decisions are no longer in force.
[46] Ratified by Ireland on 28.11.1996;
[47] Ireland ratified the ECMA 1-P on 28.11.1996 and the ECMA-2P on 26.07.2011.
[48] Ratified by Ireland on 23.08.2020;
[49] Declaration contained in a Note verbale from the Permanent Representation of Ireland, dated 26 July 2011, deposited with the instrument of ratification on 26 July 2011.
[50] The US Department of Justice, *Cloud Act Resources* (2022), available at https://www.justice.gov/dag/cloudact.
[51] The Council claims that it is an exclusive competence for the European Union, so Members can't conduct the negotiations with US on their own. See Opitek and Choroszewska, 'Uzyskiwanie dowodów cyfrowych z zagranicy w sprawach karnych – stan obecny i procedowane zmiany (część II)', 10-11 *Prokuratura i Prawo* (2020), at 7.

Why are Ireland and the United States clearly specified in this paper? The answer is simple. As mentioned above, Meta Platform, Inc. is headquartered in Menlo Park, USA. However, Meta Applications' users outside of the US and Canada sign a contract with Meta Platforms Ireland Limited, located in Dublin, Ireland. The necessity of issuing requests to them via traditional MLAT channel makes the process time consuming[52] and ineffective.[53] Because of that, authorities use other, often informal, ways of collecting e-evidence. They issue requests directly to META, for instance by using special form available on the website.[54] Authorities of UE Members sent 124 343[55] requests from January 2020 to June 2021.[56] To date, 80% of them came from Germany, France, Poland and Italy. By comparison, Eurojust registered about 3 300 cases dealing with EIOs between May 2017 and December 2020.[57] Some data was produced in case of 67% of requests executed by META. It is a quite satisfactory result, but it does not mean that authorities got all requested data. Experience has shown that META often provides partial information[58] and does not explain limitations of data access.[59] However, according to information gathered by Eurojust and Europol, there are following reasons for refusal or delay of direct requests:[60] an absence or an incorrectness of the legal basis, a wrongly addressed receiver, procedural mistakes, a lack of details and a lack of requested data.[61] Furthermore, there are no standardized UE rules concerning that kind of cooperation between service providers and public authorities, so the situation differs in various Member States. In fact, an execution of issued requests depends on the provider's willingness to cooperate.[62] Because of that, the existence of some doubts about the

[52] For example, it takes usually from 8 to 15 months for the US response. See Opitek, 'Wybrane aspekty pozyskiwania dowodów cyfrowych w sprawach karnych', 7-8 *Prokuratura i Prawo* (2018), at 8.

[53] Data access is denied, delayed or incomplete in 85 % of all requests to non-UE countries. Data access is denied, delayed or incomplete in 75 % of all MLAT requests within UE Members. See Commission Staff Working Document of 18 April 2018, SWD (2018) 118 final, at 259.

[54] Meta, *Law Enforcement Online Requests (2022),*available at https://www.facebook.com/records/login/.

[55] UK's requests sent on Janauary 2020 aren't included.

[56] This amount includes also traditional MLAT requests. The calculation was based on data available on website: https://transparency.fb.com/data/government-data-requests/.

[57] Eurojust, Report on Eurojust's casework in the field of the European Investigation Order, 2020/00269, 24 November 2020*,* at 5; Eurojust, Eurojust Annual Report 2020 Criminal justice across borders, 2021/00253, 23 March 2021, at 11.

[58] SIRIUS, SIRIUS EU Digital Evidence Situation Report 3rd Annual Report, 24 November 2021, at 22.

[59] It is important to mention that data stored by META contains many kinds of information but port numbers are not included.

[60] SIRIUS, *supra* note 59, at 61 – 64.

[61] This situation may result from expiry of the retention period, which differs among UE Members. Data retention subject has been analyzed by the Court of Justice of the EU (CJEU). The CJEU originally established a rule that a general and indiscriminate retention of traffic and location data is precluded (Joined Cases C-203/15 and C-698/15, *Tele2* and *Watson* (EU:C:2016:970). Later this principle was reconfirmed, however the Court has allowed for the possibility of various exceptions. See Case C-623/17, *Privacy Int*. (EU:C:2020:790); Case C-511/18 *La Quadrature du Net* (EU:C:2020:791); Case C-746/18 *H.K. v. Prokuratuur* (EU:C:2021:152). Nevertheless, in the opinion of the CJEU, data retention should be restricted only to serious offences.

[62] M.Böse, *An assessment of the Commission's proposals on electronic evidence Policy* (2018), at 6 and 8.

admissibility of information received through this process is justified. On the other hand, in most EU countries (about 70%) it can be entered as evidence in court. But, it means that there also EU Members, where using data obtained directly from above-mentioned providers is forbidden (e.g. Slovakia[63]) or uncertain (e.g. Poland[64]).

Why is access to data stored by META so important? Firstly, Meta Applications (especially Messenger and WhatsApp) have become common tools used to commit crimes such as fraud or child sexual abuse. Secondly, Meta Applications (especially Facebook and Instagram) are virtual places, where the offences such as threats, incitement, harassment, stalking or insult are directly committed. Thirdly, these providers are used as communication channels by criminals. In 2019 Cisco Talos found 74 Facebook groups in which stolen credit card numbers and bank account details were being openly traded.[65] Finally, since META has almost 3.6 billion monthly active users,[66] it is a big source of information about suspects in criminal cases. In accordance to SIRIUS Report, e-evidence provided by META was essential for some serious investigations related to terrorism, murders and child sexual abuse.[67]

IV. Proposal for the Regulation

Undoubtedly, the instruments mentioned above determine merely fragmentary organizational frames of procedures of effective and safe obtaining of e-evidence.

First attempts to solve the growing problem of sourcing e-evidence were made in 2016, when the Council presented conclusions on the European Judicial Cybercrime Network.[68] It was noticed, that cybercrime was one of the fastest growing forms of crime, and pointed out that mutual legal assistance procedures related to electronic data had to be accelerated and streamlined. On the other hand, these new enhanced methods of conducting criminal proceedings in cyberspace had to respect fundamental rights frameworks of affected persons.[69]

Eventually, in 2018, by virtue of article 82 the Treaty on the Functioning of the European Union (TFEU), the EC presented a proposal, which should have been a complex

[63] SIRIUS, *supra* note 59*,* at 32.
[64] Opitek, *supra* note 53, at 5.
[65] J. Schultz, *Hiding in Plain Sight,* 5 April 2019, available at https://blog.talosintelligence.com/2019/04/hiding-in-plain-sight.html.
[66] J. Wise, *Meta Platforms Inc Statistics 2022: Revenue, Users, Acquisitions & Shares* (2022), available at https https://earthweb.com/meta-statistics/.
[67] SIRIUS, *supra* note 59 , at 13 – 15.
[68] The Justice and Home Affairs Council, Council conclusions on the European Judicial Cybercrime Network, 9 June 2016.
[69] EC Report of 20 July 2021, Document 52021DC0409.

answer for demands, both decision-making bodies of the EU and the Member States. It was known under the name of *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters* (further as 'the Regulation').[70]

Contrary to the instruments described before, that proposal was presupposing the use of the highest rank legal act in the EU, which is regulation.[71] An essential issue requiring draw attention to was the fact, that both the EC and the EP were and they still are in complete agreement in the matter of what type of legal act is supposed to be used to solve a problem of obtaining e-evidence.

In the proposal itself, the EC presented a new approach to definition and understanding particular terms, which are used in the context of obtaining evidence material localized in the web and generated in a digital environment. By creating the catalogue of legal definitions[72] which are used in the proposed Regulation, that act also described a circle of subjects and the scope of data falling within the Regulation.

Crucial from the point of view of the discussed issue, is an explanation of what digital evidence material actually is. Assumedly, it is supposed to mean material that has been gathered in digital form, stored by or on behalf of a service provider, at the time of receiving of the European production or preservation order. It is including subscriber data, access data, transactional data and content data.[73]

According to terms of the Regulation, offering services in the UE, beyond enabling using them in one or more Member States, means also having a substantial connection to such a state. It is connected directly with key (from the point of view of discussing issue) article 3 (1) of the proposal. In that part of regulation, it has been stated that it has to be applicable to those of providers who have not held their headquarters at any of Member States, but offering their services in such a state. Those conditions are referred to providers who are localized in Europe as well as beyond the continent. It is significant insomuch as a matter of the cross-border character of crimes committed with using of computer technology, as well as a benefaction of contemporary times in the shape of social media, a still high percentage of data

[70] EC Proposal of 17 April 2018, Document 52018PC0225.

[71] Existing instruments and using them usually have come down to creating new solutions in the way of directives or applying existing rules of conventions. That kind of practice has been used in the case of the European Arrest Warrant, the EIO or the CCC. A notable exception, corresponding strictly to TFEU, had been the establishment of EUROPOL and EUROJUST in the way of regulations (art. 85 and 88 TFEU).

[72] A conceptual framework was included and developed in art. 2 of the Regulation.

[73] EC Proposal, *supra* note 70, Art. 2 (6). Particular types of data have been defined in the following points (7-10) of the mentioned article.

which are fundamental for proper criminal proceedings remains in the disposition of subjects with global extent such as Facebook.

Instrument used to obtain data mentioned above, which had been proposed by the EC is European Production and Preservation Orders for electronic evidence in criminal matters (further as EPO and EPO-PR). Assumedly, these options are supposed to be as universal as possible and be adaptable to the legal procedures of Member Countries and technological reality. Especially it is supposed to be a tool to avoid trespass on the jurisdiction of another state in a way that is not legally acceptable. The first of the orders, according to the project, is a binding decision of the authority of a Member State, issued for a provider offering services in the EU and established or represented in another Member State, imposing an obligation to produce electronic evidence stored by such provider or on his behalf. On the other hand, EPO-PR is understood as a binding decision of the authority of the Member State, issued for provider offering services in the EU and established or represented in another Member State, impose an obligation to preserve of electronic evidence stored by such provider or on his behalf, for a purpose of subsequent request of production those materials.[74] Both of those orders, as investigative measures, may be issued in criminal investigations as well as judicial proceedings. Furthermore, they might be issued for a legal person. However, they cannot be issued in connection to services offered beyond the EU or others that have not been defined in article 2 (3) of the Regulation.

In regard to the procedure of issuing of both orders, the mandatory presence of judicial authorities must be pointed out, operating as an issuing authority or a validating authority. In the case of the EPO, exclusive competence to issuing the decision regarding some categories of demanded data might have only judicial authorities. However, in case of those demands that do not include transactional data or content data, and are referred to subscriber data or/and access data, orders may be issued also by the public prosecutor, without the necessity of obtaining subsequent approval of judicial authorities.[75]

Frames for issuing of both instruments are determined by proportionality to the legitimate pursued aim and necessity in the scope of a particular, individual case. Moreover, orders should be used only if domestic law allows the deployment of similar instruments in a comparable domestic case in the issuing State when cross-border collecting of evidence material is not required.[76] The possibility of issuing those orders is also coming down to the

[74] EC Proposal, *supra* note 70,Art. 2 (1) and (2).
[75] EC Proposal, *supra* note 70, Art. 4.
[76] EC Proposal, *supra* note 70, Art. 5 and 6.

connection with the specific types of crimes. While in case of the EPO regarded with subscriber data and access data, the Regulation does not create limitations in terms of types of crimes, in case of the rest of categories of data, such order may be issued exclusively in relation to crimes which maximum adjudicate custodial sentence is at least 3 years or in relation to criminal offenses specified in the framework decision and directives pointed in article 5 (4) of the Regulation.

Both orders should be pursued by issuing a proper certificate (a European Production or Preservation Order Certificate – further EPOC or EPOC-PR) and transmitting it to the proper addressee defined according to article 7 of the Regulation. What is important from the point of view of fluent realization of an order, the project of the Regulation assumes strict date limits of the execution of both orders.

In the case of the EPO, the addressee of the certificate should realize it and transmit to issuing authority or the law enforcement authorities at the least within 10 days without further delay, unless authority mentioned above indicates reasons determining shorter terms of realization. In emergency cases, understood according to article 2 (15), data should have to be transmitted immediately, at least within 6 hours.

Much too controversial solution proposed by the EC is a possibility of refusal to execute the order by the addressee in case of considering that certificate and the demand might violate the Charter of Fundamental Rights of the European Union or violation of law is manifestly abusive. Although the Regulation projects strict procedures in such cases, giving such competencies to non juridic subjects is highly hazardous, especially when it comes down to *ius cogens*.[77]

In relation to the EPO-PR procedure of preserving data is different. An addressee of the certificate, without delay, after its receiving, preserve requested data for a period of time no longer than 60 days. After an ineffective expiration of a term, preservation is extinct.

An important matter, differentiating potentially real effectiveness of the discussed regulation from existing legal measures, is the possibility of enforcement of execution of orders under penalty of a fine. In terms of that, an issuing authority analyzes the reasons for non-execution of a certificate by itself, and in case of considering reasoning as inconclusive,

[77] An important question is the lack of consequence of the legislator. In case of those demands of data, which interfere so much in the sphere of civil liberties and the protection of personal data in the meaning of article 16 of TFEU, the Regulation gives exclusive competence to issue the certificate to the court of competent justice. On the other hand, the same regulation gives an addressee (which is deprived of competencies belonging to the judiciary) an opportunity of secondary verification and analyze the legitimate aim of the certificate. In this regard, one can risk the statement that, in the same field, which judicial authorities are exclusively competent to issue the certificate, their capability of making the right decision and the proper conclusion is questioned.

may implement procedures engaging the so called enforcing authority. In case of lack of activity of addressee, enforcing authority, according to its national law may impose a pecuniary sanction.

The proposal mentioned above has been passed down to the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament. On December 11, 2020 *the report on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*,[78] including propositions of amendments and results of voting on the project has been presented. According to that report, solutions proposed by the EC have been mostly rejected *a limine* or changed to such an extent that, one may risk a statement; the new, alternative project of the regulation has been created.

It has been reasonably pointed out that projected instruments should be proportionate to the legitimate pursued aim. There is no doubt, which also had not gone unnoticed by the EC and parliamentary committee, that a solution, whatever will be, must be effective and what is most important, practical. Nonetheless, it is connected with far-reaching consequences and interference in the sphere of peremptory laws and essential matters, including the right to protection of personal data that is mentioned in article 16 TFEU.

In terms of principal issues, the scope of the definitions has been changed, especially the definition of electronic evidence material, which has been replaced by the term 'electronic information'.[79] Furthermore, the project of regulation has been complemented by bringing the institution of legal representative of service provider offering services in Member States and not having its legal address.[80] According to article 6a, a legal representative shall be established in one of the Member States where the service provider offers its services. Such legal representatives act on behalf of providers. Furthermore, they might be held accountable for failing to fulfill the obligations.

Proposed changes also include the obligation of notification, which strictly means, that beyond transferring a certificate to the addressee, issuing authority must notify the appropriate authority in the state of execution of the orders. In regard to the above, the catalogue of

[78]EP Report of 11 December 2020, A9-0256/2020.
[79] EC Proposal, *supra* note 70, Art. 2(6).
[80] First attempts to establish an institution of legal representative had been made in 2018 when the Commission Proposal for the EP and Council Directive of 17 April 2018 laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM (2018) 226 was published. For the last time, the Proposal was discussed in the Council in March 2019. Since then, no efforts were made to move forward with the legislative procedure.

premises grounding for a refusal of execute orders have been extended. The difference is that those competencies have been given to execution authorities, according to article 10a.

The proposal for the Regulation has gained acceptance in the European juridical scene.[81] There is no doubt, the matter of gathering digital evidence, positioning it into the criminal proceedings, as well as protection and respect for human rights in the midst of all of it (also suspects and defendants), is an important case to such a degree, that even the Member States, hitherto reluctant in terms of relinquish right to self-determination to a degree and rejecting possibilities creating by the EU, have decided to adhere, firstly by negotiations about solutions, and the next (under the condition that the project is still the proposal of regulation) implement effects of collaboration to national legal orders.[82]

V. A critical look at the e-evidence Regulation draft.

Having presented the provisions of the e-evidence Regulation, we shall move on to the analysis of those provisions, and also of the modifications that were added to the proposal during the trilogue process. The question is: does the e-evidence Regulation have a chance of bringing evidence gathering procedures into the 21st century, as it was originally envisioned?

Starting with the definitions laid down in the proposed Regulation,[83] it is our belief that the proposed understanding of 'offering services in the Union' has been properly designated. The fact that the proposal uses two conditions that were described above is crucial, as it leaves no doubt that a service provider cannot benefit from offering its services in the Union, without at the same time having to accept the general responsibility to provide evidence. Additionally, the understanding of 'substantial connection'[84] includes having a significant number of users in at least one Member State. That guarantees that the big players, such as Meta, will definitely fall under the definition and that they will be obliged to follow the Regulation.

---

[81] See Tosza, 'The European Commission's Proposal on Cross-Border Access to E-Evidence. Overview and Critical Remarks', 4 *EUCRIM. The European Criminal Law Associations' Forum (EUCRIM)* (2018*)* 212; Blažič and Klobučar, *supra* note 21; Laurits, 'Regulating the Unregulatable: An Estonian Perspective on the CLOUD Act and the E-Evidence Proposal'*,* 29 *Juridica International* (2020) 62.

[82] Particular attention is supposed to be drawn to Ireland which, under rules of Protocol no. 21 on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice (OJ 2016 C 202/295), usually does not participate in the adoption by the Council of proposed measures related to title V of Part Three of TFEU. In point 64 of the preamble of Project of Regulation proposed by Committee on Civil Liberties, Justice and Home Affairs, had been presented a clear statement of Ireland about the intent of acceding to the Regulation. It is crucial laps from, nearly always used by Ireland, protocol no. 21.

[83] EC Proposal, *supra* note 70, Art. 2.

[84] The evolving proposal has also narrowed down what is to be understood as a substantial connection; see EP Report of 11 December 2020, A9-0258/2020.

However, other definitions could lead to multiple practical issues down the road. This applies especially to the various types of data defined in the Regulation. These definitions have been narrowed down and polished during the trilogue process, resulting in the split into 'subscriber', 'traffic' and 'content' data.[85] It has been justifiably argued that the primary aim of any definition of data in the context of electronic evidence should, above all else, be comprehensive and leave no legislative gaps. At the same time, it should be focused on legal aspects from the perspective of the fundamental rights of the affected person.[86] While the proposed definitions seem to meet these requirements, they could bring other issues. For one, the practitioners in law enforcement, prosecutors and judges are not usually educated in computer science and therefore could face some difficulty in identifying the various types of data. This applies especially to 'traffic data', which is the most technical in its description by far. It is also necessary to mention that multiple Member States do not have a specific definition for electronic evidence[87] and could see the new provisions as limiting when it comes to obtaining such evidence.

Another part of the proposal connected directly to the data definitions is the status of the issuing authority of the EPO. The evolved proposal establishes that a public prosecutor may only issue an EPO for obtaining subscriber data and IP addresses for the sole purpose of determining the identity of specific persons with a direct link to the relevant criminal proceedings.[88] To request any other types of data, the EPO must be issued or approved by a judge or a court.[89] It is necessary to point out that the EIOD left the question of who may issue the order to the Member States, while the proposed Regulation provides unified provisions in this matter when it comes to the EPO.[90] The aim of this new provision is undoubtedly to guarantee the basic rights of the person whose data is being acquired. However, some member states, including Poland, do not require court approval for obtaining electronic evidence in their domestic legal systems, leaving that decision to the public prosecutor during the pretrial phase. In this case, we are worried that this limitation could simply lead to some countries preferring to still use EIO instead of entering a potentially lengthy process of obtaining court approval to request data, thereby ruining the very purpose of EPO. One could argue that this danger is alleviated by the provision that obtaining IP addresses does not require a court's

[85] Ibid. Art. 2 (7 - 9).
[86] Warken, '*Classification of electronic data for criminal law purposes'*, 4 *EUCRIM* (2018) 226.
[87] SIRIUS*, supra* note 59, at 48 – 52.
[88] Normally, an IP address would be considered 'traffic data'.
[89] EP Report, *supra* note 84, Art. 4.
[90] Tosza, 'All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order', 11 *New Journal of European Criminal Law* (2020) 161.

approval. However, in our practical experience we have found that an IP address is almost never enough to identify a person during an investigation, and other crucial data is also necessary, such as 'time of communication' (which is considered 'traffic data').

It also needs to be emphasized that the correct choice of legislative instrument was chosen for the e-evidence proposal – a regulation. This is most certainly the most advantageous move from the point of legislative strategy. A regulation has general application, binding in its entirety, and is directly applicable in all Member States, in contrast to a directive, which is binding only according to its aim and results and needs separate implementation in each Member State.[91] In addition, a positive move from the trilogue process comes from the proposal to include the service provider legal representative provisions in the regulation itself, rather than in a separate directive.[92] As legal representatives are needed to guarantee that service providers based outside of the Union can effectively comply with EPOs, this issue should not be regulated separately. It is also worth noting that service providers will be obliged to establish a representative in one of the Member States bound by the regulation, so they will not be able to avoid its provisions. However, the Regulation should go further when it comes to sanctions the providers could face if they refuse to cooperate with the provisions of the Regulation,[93] as it was done in the case of the GDPR.[94] The provision regarding sanctions should be more precise and direct, as it is desirable that sanctions in various Member States are similar. Otherwise, providers may try to deliberately establish their representative in a Member State that will have established the most lenient sanctions.

One of the more controversial issues is that of the addressee of EPO and of notification. The original legislative proposal established that EPO would be addressed directly to the service provider, and not to the executive authority. The executive authority played an important role, but not if the EPO could be executed without issues. In those cases, the involvement of the executing authority was not required at all. The amended proposal laid down by the EP does not accept that, and establishes that EPO is to be addressed to both the provider and the executing authority.[95] The aim of this provision is to further guarantee the basic rights of the affected persons, as the executing authority may refuse to let the provider

[91] Art. 288 TFEU.
[92] EP Report, *supra* note 84, Art. 6a.
[93] The proposal states that Member States shall lay down rules on the sanctions, and that they shall be effective, proportionate and dissuasive - EP Report, *supra* note 84, Art. 6a (9) and Art. 13 (1).
[94] Administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher – article 83 of the EP and Council Regulation 2016/679, OJ 2016 L 119/1.
[95] EP Report, *supra* note 84, Art. 7, Art. 8a and Art. 9.

carry out the order.[96] However, this kind of solution has been criticized by the representative of some Member States, who have expressed serious doubt,[97] pointing at the fact that this solution effectively strips EPO of any truly new value over existing instruments. In our view, this is indeed the case. Direct cooperation between the issuing authority and the service provider was perhaps the single most important aspect separating the EPO from the EIO.[98] It is difficult to imagine that the new instrument can truly achieve its purpose without being significantly simpler in its application compared to existing measures, most notably the aforementioned EIO. Above all, the simultaneous notification seems to disregard the idea of mutual trust between the Member States and their judicial systems. It is our fear that, with the abandonment of enhanced mutual trust, the purpose of the Regulation may be lost. It is however worth noting that the final provisions regarding notification are still being discussed by all the stakeholders, with signs that a compromise might be reached.[99] We agree with the conclusion that further work should focus on reconciling the views of the EC and the Council with the views of the EP, as lack of balance and too much focus on protective measures could hinder the efficiency of the new instrument.[100]

Another very controversial part of the proposal that has also been met with criticism is the right of the service provider to refuse to execute an order, based on its own conclusion that it manifestly violates the Charter of Fundamental Rights of the European Union, or – in the EP's amended proposal – that it is in general manifestly abusive or that it exceeds the purpose of the order.[101] Some Member States have gone as far as to call this an example of 'privatization of criminal law'.[102] The main argument against this provision is that service providers lack the necessary competence to decide if an order issued by a judge, a court or a public prosecutor should be considered abusive in the context of basic rights. The EP's proposal seeks to mitigate this somewhat, leaving it to the executing authority to seek necessary clarification from the issuing authority regarding the order. Once again, this provision seems to stem from a lack of belief in the idea of mutual trust between Member

[96] Ibid. Art. 8a, Art.10a.
[97] Opitek and Choroszewska, 'Uzyskiwanie dowodów cyfrowych z zagranicy w sprawach karnych – stan obecny i procedowane zmiany (część II)', 9 *Prokuratura i Prawo* (2020).
[98]Tinoco-Pastrana, 'The Proposal on Electronic Evidence in the European Union', 1 *EUCRIM* (2020) 44; Tosza, *supra* note 90.
[99]L. Bertuzzi, *Council document hints at progress on cross-border electronic evidence,* 22 October 2021, available at https://www.euractiv.com/section/data-protection/news/council-document-hints-at-progress-on-cross-border-electronic-evidence/.
[100] Corhay, 'Private Life, Personal Data Protection and the Role of Service Providers: The EU e-Evidence Proposal', 6 *European Papers* (2021) 441.
[101] EC Proposal, *supra* note 70, Art. (9) 5; EP Report, *supra* note 84, Art. 9(5).
[102] Opitek and Choroszewska, *Uzyskiwanie (...) I, supra* note 98.

States, which should be the very basis of all mutual legal cooperation. Therefore, this particular provision seems more likely to hinder the efficiency of criminal proceedings rather than help protect basic rights. Furthermore, we are worried that it could be used by some service providers as their basic response, in an attempt to discourage European judicial authorities from demanding data that is in their possession.

Another significant modification from the original Regulation project is in Article 11, which deals with the question of the order's confidentiality. Originally, this provision was clearly focused on the service provider's duty to keep the order confidential from the affected person. Any issuing authority could request that the service provider refrain from informing that person for as long as necessary to avoid obstructing the relevant criminal proceedings. The evolved Article 11 instead makes it a rule that the person whose data is being sought is to be informed without undue delay, and any exception to this rule can only be made through a separate judicial order provided by the issuing authority. However, based on our practical experience, we are worried that this exception will become the general practice. Issuing authorities will almost always have to seek the judicial order of confidentiality, because the pretrial investigation must remain secretive. We have noticed that e-evidence is almost always sought as a tool for the identification of a perpetrator, who obviously must not be alerted to the possibility that he or she is being traced.

It is also necessary to mention the burning issue that is especially important for the service providers, and that is the potential conflict with third country law. The Regulation provides that a potential conflict may be brought up by both the executing authority and the service provider itself.[103] The procedure laid down in this case is quite complex and lengthy. It includes multiple exchanges of information and of positions, and ultimately, the decision whether the order shall be executed is left with the executing authority. It has, however, been somewhat streamlined and simplified compared to the original proposal,[104] which provided that the decision would be left with the court of the issuing Member State. This can definitely be seen as a move in the right direction; however, on the other hand it once again brings EPO closer to the nature of the EIO, which may limit the usage of the new instrument. In our opinion, this part of the Regulation may require some additional work. On one hand, it has been correctly pointed out that service providers may find themselves in a situation of a conflict of interests: whether to follow EU law and face potential repercussions on the grounds of their domestic law (for example, to face lawsuits from American natural and legal

[103] EP Report, *supra* note 84, Art. 14a.
[104] EC Proposal, *supra* note 70, Art. 15.

persons in case of the tech giants based in the United States).[105] On the other hand, as it was already mentioned – service providers benefit greatly from being able to offer their services in the EU and therefore should not be able to avoid following the EU law when it comes to providing evidence for criminal proceedings dealing with crimes committed on European citizens.

Finally, the one aspect of the proposed regulation that is most certainly positive and moving in the right direction is the default time of 10 days the provider has to transmit the data.[106] However, with all the additional procedures and safeguards mentioned above, it remains to be seen whether the average EPO will in fact be realized in such a short time.

VI. Conclusions

As it was outlined above, the evolution of mutual legal assistance will soon take another step: this time with the aim of targeting e-evidence specifically. What is unquestionable is that the general idea of the e-evidence Regulation is a very good one, as it aims to create a legal framework that would oblige service providers present in the UE to produce e-evidence on demand of a judicial authority from any Member State. However, is unclear whether this revolutionary regulation can actually achieve that purpose and correctly balance efficiency of investigation and protection of basic rights. We believe that the right to privacy is, as important as it should be, may in practice diminish the rights of victims of cybercrimes. Moreover, if EPO fails to become the new universal tool for gathering e-evidence, then the current phenomenon of unregulated cooperation with tech giants, such as Facebook, will continue, leading to more legal uncertainty.

Bibliography

1. The European Convention on Mutual Assistance in Criminal Matters 1959, ETS 030.
2. Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters 1978, ETS 099.
3. OJ 2000 L 239/19.
4. OJ 2000 C 197/3.
5. OJ 2001 C 326/2.
6. Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters 2001, ETS 182.

[105] Opitek and Choroszewska, *Uzyskiwanie (...) II, supra* note 51.
[106] EP Report, *supra* note 84, Art. 8a (2).

7. Convention on Cybercrime 2001, ETS 185.
8. Blažič and Klobučar, 'Removing the barriers in cross-border crime investigation by gathering e-evidence in an interconnected society', 29 *Information & Communications Technology Law* (2020) 66, at 68.
9. OJ 2003 L 196/45.
10. OJ 2008 L 350/72.
11. Directive 2014/41/EU, OJ 2014 L 130/1.
12. Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence 2022.
13. Council of Europe Portal, *New Treaties* (2022), available at https://www.coe.int/en/web/conventions/new-treaties.
14. The US Department of Justice, *Cloud Act Resources* (2022), available at https://www.justice.gov/dag/cloudact.
15. Opitek and Choroszewska, 'Uzyskiwanie dowodów cyfrowych z zagranicy w sprawach karnych – stan obecny i procedowane zmiany (część II)', 10-11 *Prokuratura i Prawo* (2020).
16. Opitek, 'Wybrane aspekty pozyskiwania dowodów cyfrowych w sprawach karnych', 7-8 Prokuratura i Prawo (2018).
17. Commission Staff Working Document of 18 April 2018, SWD (2018) 118 final.
18. Meta, *Law Enforcement Online Requests* (2022), available at https://www.facebook.com/records/login/.
19. Eurojust, Report on Eurojust's casework in the field of the European Investigation Order, 2020/00269, 24 November 2020.
20. Eurojust, Eurojust Annual Report 2020 Criminal justice across borders, 2021/00253, 23 March 2021.
21. SIRIUS, SIRIUS EU Digital Evidence Situation Report 3rd Annual Report, 24 November 2021.
22. M.Böse, *An assessment of the Commission's proposals on electronic evidence Policy* (2018).
23. J. Schultz, *Hiding in Plain Sight,* 5 April 2019, available at https://blog.talosintelligence.com/2019/04/hiding-in-plain-sight.html.
24. J. Wise, Meta Platforms Inc Statistics 2022: Revenue, Users, Acquisitions & Shares (2022), available at https https://earthweb.com/meta-statistics/.

25. The Justice and Home Affairs Council, Council conclusions on the European Judicial Cybercrime Network, 9 June 2016.
26. Commission Report of 20 July 2021, Document 52021DC0409.
27. EC Proposal of 17 April 2018, Document 52018PC0225.
28. EP Report of 11 December 2020, A9-0256/2020.
29. Tosza, 'The European Commission's Proposal on Cross-Border Access to E-Evidence. Overview and Critical Remarks', 4 *EUCRIM. The European Criminal Law Associations' Forum (EUCRIM)* (2018) 212.
30. Laurits, 'Regulating the Unregulatable: An Estonian Perspective on the CLOUD Act and the E-Evidence Proposal', 29 *Juridica International* (2020) 62.
31. OJ 2016 C 202/295.
32. EP Report of 11 December 2020, A9-0258/2020.
33. Warken, 'Classification of electronic data for criminal law purposes', 4 *EUCRIM* (2018) 226.
34. Tosza, 'All evidence is equal, but electronic evidence is more equal than any other: The relationship between the European Investigation Order and the European Production Order', 11 *New Journal of European Criminal Law* (2020) 161.
35. Opitek and Choroszewska, 'Uzyskiwanie dowodów cyfrowych z zagranicy w sprawach karnych – stan obecny i procedowane zmiany (część II)', 9 *Prokuratura i Prawo* (2020).
36. Tinoco-Pastrana, 'The Proposal on Electronic Evidence in the European Union', 1 *EUCRIM* (2020) 44;
37. L. Bertuzzi, *Council document hints at progress on cross-border electronic evidence,* 22 October 2021, available at https://www.euractiv.com/section/data-protection/news/council-document-hints-at-progress-on-cross-border-electronic-evidence/.
38. Corhay, 'Private Life, Personal Data Protection and the Role of Service Providers: The EU e-Evidence Proposal', 6 *European Papers* (2021) 441.