Articles

Articles / Aufsätze

Fil Rouge

The European Union already has an impressive track record when it comes to the protection of its citizens' data. Yet the challenges posed by the digital revolution are not limited to protecting people's privacy, but also require finding effective ways to access data when need be, including for criminal investigations. The lack of a comprehensive framework in that respect currently results in more informal solutions based on the voluntary cooperation of service providers, not necessarily with due regard to the protection of fundamental rights. This problem is also a good example of a broader phenomenon linked with the technological revolution: the role of service providers as partners in law enforcement. Their role is not only instrumental in the gathering of e-evidence, but also, for instance, in the fight against the dissemination of illicit content online.

The contributions in this issue of *eucrim* touch upon all these difficulties. The first two articles – by *S. Tosza* and by *J. Daskal* – deal with the same problem: law enforcement access to data held by service providers for the purpose of criminal investigation. As data is very often held in a different country than the place of criminal investigation, the complexity of instruments necessary to obtain such data is out of proportion. *S. Tosza* presents the EU initiative aimed at creating a legal framework for direct requests for electronic evidence sent by law enforcement authorities in the EU to service providers in another EU Member State (the "e-evidence initiative"). *J. Daskal* discusses the recent changes in U.S. law, which should facilitate the transfer of data from U.S. service providers to authorities in the EU.

The immense growth in data-analysing capacities has thrown into question the traditional classification of data, as even non-content data may be extremely revealing when gathered in sufficient quantity and properly analysed. *C. Warken* critically analyses the current approach to classifying data and proposes a new take on the matter.

G. Robinson examines the European Commission's proposal for a Regulation on preventing the dissemination of terrorist content online. This highly relevant initiative largely relies on the good cooperation of service providers, including their proactive role.

Katalin Ligeti, University of Luxembourg and eucrim Editorial Board Member & Stanislaw Tosza, University of Utrecht

The European Commission's Proposal on Cross-Border Access to E-Evidence

Overview and Critical Remarks

Dr. Stanislaw Tosza

With human activity becoming more and more dependent on digital technologies, criminal investigations increasingly depend on digital evidence. Yet the gathering of this type of evidence is far from straightforward. Besides technological challenges, one of the major obstacles that law enforcement authorities encounter is the fact that the data they need is often stored abroad or by a foreign service provider. At the 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 length of the procedure when resorting to the EIO is far too slow, because relevant data can be lost in the meantime. This article discusses the initiative of the European Commission to establish a European legal framework regarding direct requests for electronic evidence sent by law enforcement authorities in the EU to service providers in another EU Member State (the "e-evidence initiative"). The initiative, which is currently under debate in the EU Parliament after the Council agreed on proposed amendments, is not without controversy. The article analyses its overall structure and the most important aspects of its design, and it offers critical remarks on several major elements of the initiative.

I. Introduction

A large number of criminal offences, not only cybercrime, is currently committed in a way that leaves digital traces that can serve as evidence. In order to effectively investigate and prosecute these offences, law enforcement must have access to digital data, which is mostly in the possession of service providers, often located abroad. The law of criminal procedure allows the authorities to access this data, while protecting suspects' procedural safeguards. However, when the service provider is located in another country or the data is stored abroad, law enforcement should in principle resort to mutual legal assistance (MLA) because their coercive powers are limited to their national territory.

As the significance of digital or electronic evidence has grown, so has the frustration of law enforcement with the cumbersome procedure to acquire this data in combination with the number of cases when digital evidence is needed and the relevant data is held abroad. This has stimulated attempts to find unilateral solutions forcing providers to deliver data not stored in the territory of the requesting state circumventing the MLA procedure, which resulted in significant litigation,[1] and calls for reform of the framework. The latter is not an easy undertaking, as the complexity of the issue is composed of problems linking criminal procedure, international law, in particular questions of jurisdiction and sovereignty in the context of criminal investigations, EU law as well as the impact of fast developing technology, in particular cloud computing or encryption.[2]

With the Conclusions of 9 June 2016 the JHA Council requested the Commission to develop a legal framework that would allow law enforcement to obtain relevant data.[3] This request led to the proposal of the Commission of 17 April 2018 that is composed of two instruments: a regulation and a directive.[4] The aim of this contribution is to provide an overview of and a few critical remarks on the Commission's proposal, in particular focusing on the draft regulation, which is the main component of the legislative initiative.

At the same time, legislative work has also progressed in the U.S., with the ultimate adoption of the CLOUD Act in March 2018, which is meant to facilitate access to data held by U.S. companies by non-U.S. law enforcement authorities. This act is the subject of the contribution by *Jennifer Daskal* in this issue of eucrim.

II. Commission's Proposal

The envisaged regulation would create two new instruments: a European Production Order (EPdO) and a European Preservation Order (EPsO).[5] An EPdO is defined as "a binding decision by an issuing authority of a Member State compelling a service provider offering services in the Union and established or represented in another Member State, to produce electronic evidence" (Art. 2(1) of the draft regulation[6]). An EPsO is "a binding decision by an issuing authority of a Member State compelling a service provider offering services in the Union and established or represented in another Member State, to preserve electronic evidence in view of a subsequent request for production" (Art. 2(2)). It is interesting to note that an EPsO may result not only in an EPdO, but also for instance in a mutual legal assistance request or a European Investigation Order (Art. 6(2)).

The crucial characteristic of the Commission's proposal is that the orders goes from the issuing authority in one Member State directly to the service provider in another Member State and the data should go back the same way. The involvement of an authority in the executing state is, in principle, avoided and the basic check of the order is done by the service provider. In order to guarantee the effectiveness of the regulation, the second piece of the Commission's proposal, i.e. the directive, obliges the Member States to provide for a framework assuring that there is a known and empowered legal representative of a service provider to whom the order may be addressed. The choice both of the legal basis and of the legal instrument is noteworthy: The directive, which must be transposed by the EU Member States, has an internal market legal basis (see also 2. below), whereas the – binding and directly applicable – regulation is based on Art. 82(1) TFEU, which provides for judicial cooperation in criminal matters on the basis of the mutual recognition principle. While being a regulation, a number of issues will have to be clarified by national law, most notably sanctions and remedies (see below).

1. Draft Regulation

a) What may an order be issued for?

The EPdO and the EPsO have the same objective: they oblige the service provider to respectively produce or preserve electronic evidence. The term "electronic evidence" is explained in Art. 2(6). This definition is characterised by three elements: Firstly, evidence must be stored in an electronic form either by the service provider or on its behalf. Secondly, it has to be stored at the time of receipt of the EPdO or EPsO. This means that the order concerns the data that is already in the possession of the service provider and not any data to be obtained in the future, thus excluding any future surveillance. Thirdly, the term evidence is not defined as such, but the definition provides for four types of data of which that evidence might consist: subscriber data, access data, transactional data and content data.

These four categories of data are further defined in the draft regulation in Art. 2(7)–(10). The spectrum includes content and non-content data, with the latter being divided into three categories (subscriber data, access data, transactional data). In terms of infringement of fundamental rights, the regulation provides two groups of categories of data: subscriber and access data on the one hand, which are considered less intrusive, and transactional and content data, where the intrusiveness is deemed more significant. The differentiation particularly affects the possibility of using the order, which is limited to some categories of offences for the second group, whereas it is open to all offences for subscriber and access data. Furthermore, the differentiation has an impact on the radius of the action of the prosecutor's, who is excluded from the list of competent issuing authorities when it comes to transactional and content data. As per the Explanatory Memorandum to the proposal, the differentiation between the two categories is made according to the following philosophy: data related only to the identification of the user is less intrusive and can be made more accessible, whereas data involving predominantly the content of a person's activity should be more protected.[7] The Explanatory Memorandum considers that the starting point of an investigation is often the subscriber data or access data in order to reveal the identity of the suspect, before data about the content is sought.

b) Who may issue the order?

While the Member States may differ as to which authorities they give the right to ask for data from service providers in the national context, the draft proposes a quasi-harmonised approach in that regard. It should be borne in mind, that no margin of discretion is allowed, because no implementation of the provisions of a regulation is needed (see above). The Commission singled out three categories of authorities that can be entitled to issue an EPdO or EPsO (Art. 4).

The first group contains authorities that are entitled to issue both types of orders and for all types of data: judges, courts and investigative judges. The second group is composed of prosecutors whose authority is limited to what the draft considers to be less sensitive measures (cf. recital 30 of the preamble). Prosecutors may issue an EPsO for any type of data, but an EPdO only for subscriber and access data. Given the fact that a regulation (and not a directive) will be enacted, it does not seem to be possible for the Member States to restrict the circle of authorities entitled to issue the orders, e.g. by further limiting the power of the prosecutor. As a result, it may happen that a prosecutor might be in the position to issue an EPsO for content data at the European level, while he or she would not be able to do so in a purely domestic context.

The third group is defined as follows: "any other competent authority as defined by the issuing State which, in the specific case, is acting in its capacity as an investigating authority in criminal proceedings with competence to order the gathering of evidence in accordance with national law." Such orders will need to be examined for their conformity with the conditions set out for the validity of the orders. The authorities entitled to validate the order are the same two (aforementioned) groups as those for issuing the orders, according to the same range of competences (with the prosecutor's competence limited to the less intrusive types of data). In other words, the third category would include authorities that are equipped with the necessary power to gather electronic evidence according to the national laws of the Member States. Thus, prosecutors can also be entitled to ask for transactional and content data, but with the necessary authorisation and conferral of powers is at the discretion of the national legislator. The language of the draft indicates that a piece of national legislation would be necessary in this respect because, contrary to other instances (e.g. Art. 5(2)), the draft regulation does not refer to similarities with national rules or comparable domestic situations.

c) Who is the recipient of the order?

The recipient of the order is a service provider offering services in the Union and established or represented in another Member State. A service provider can be a natural or a legal person and is otherwise defined by the services it offers, which, according to Art. 2 (3), can be:

- Electronic communication services;
- Information society services;
- Internet domain name and IP numbering services.

These categories are explained in more detail in the Explana-

tory Memorandum and use also references to other acts. In practice, the first two categories (electronic communication services and information society services) comprise such services as Skype, WhatsApp, Amazon, Dropbox and mailing services.[8] As to the last category of the definition of service providers (Internet domain name and IP numbering services), the Explanatory Memorandum makes reference to the providers of Internet infrastructure services that hold data potentially of high relevance in identifying the suspect.[9]

Another requirement is that providers of the services described above fall within the scope only if they are offering services in the Union and are established or represented in another Member State. These terms are further explained in the Directive itself (Art. 2(4)) and in the Explanatory Memorandum.[10] Mere accessibility of the service from the territory of the European Union cannot be a sufficient criterion, as this would cause every provider in the world to fall within the scope. Furthermore, the service provider has to be established or represented in *another* EU Member State, since otherwise there would be a purely domestic situation, which is excluded from the scope.

An EPdO or an EPsO should be addressed directly to a legal representative that the service provider shall designate for the purpose of gathering evidence in criminal proceedings (Art. 7(1)). The efficiency of this approach is supported by the proposed Directive (see below 2.) and alternative addressees if such a representative is not designated (cf. Art. 7(2)–(4)).

d) Under what conditions may the order be issued?

The draft regulation provides for a set of common conditions for issuing EPdOs and EPsOs as well as specific conditions for each of them. The first common condition is that the order may be issued only for criminal proceedings, which includes the pre-trial and the trial phase (Art. 3(2)). According to Art. 3(2), the order may also be issued in proceedings against legal persons, where these persons may be held liable or punished. This formulation excludes any sort of double criminality requirement in this respect: even if the executing Member State does not provide for criminal liability of legal persons, the order still needs to be executed.

The second condition applicable to both orders refers to necessity and proportionality. The draft regulation distinguishes, however, between the two types of orders if it comes to the reference point of the evaluative criteria, which is founded in the different objectives of these instruments. The EPdO must be necessary and proportionate for the purpose of the criminal proceedings in question (Art. 5(2)). By contrast, the EPsO must be necessary and proportionate to prevent the removal, deletion or alteration of data in view of a subsequent mutual legal assistance request, a European Investigation Order or an EPdO (Art. 6 (2)).

Two additional conditions limit the issuing of an EPdO, both referring to the national law of the issuing Member State. First, a similar measure must be available for the same criminal offence in a comparable domestic situation. This excludes the use of the EPdO in an issuing Member State that does not provide for such a measure in this context, thus limiting the harmonising effect of the regulation and positioning the applicability of the EPdO within the realm of national law. This limiting effect must, however, be relativized: firstly, the limitation affects the power of the national authority, but not the foreign one. Secondly, the formulation does not state that the condition of application must be identical.

A second additional condition foresees that the application of the EPdO is also limited depending on the type of data and the type of offence in question. In case of subscriber or access data, the issuance of an EPdO is allowed for any criminal offence, whereas the issuing of an EPdO for transactional or content data is limited to two groups of offences. The first group refers to the national law: the EPdO may be issued for "offences punishable in the issuing State by a custodial sentence of a maximum of at least 3 years." The second one makes reference to framework decisions and directives (which harmonised substantive criminal law in specific fields) and allow national authorities to issue an EPdO regardless of the severity of punishment on the national level in the following cases:

- Fraud and counterfeiting of non-cash means of payment;
- Sexual abuse and sexual exploitation of children and child pornography;
- Attacks against information systems;
- Terrorism.

e) Execution

The EPdO or EPsO will be transmitted to the recipient through certificates.[11] The certificates are to be issued according to the models annexed to the draft regulation (Annex I and II). Some flexibility is granted as far as the transmission of the certificate is concerned. Any means are acceptable provided that they are capable of producing a written record and allow to establish the authenticity of the certificate (Art. 8).

Tight deadlines are foreseen for the execution of the orders (Art. 9). As far as the EPdO is concerned, the draft distinguishes as follows: in regular cases, the service provider should transmit the data to the issuing authority at the latest within 10 days from the moment of receiving the certificate. In emergen-

cy cases, which are defined as an "imminent threat to life or physical integrity of a person or to a critical infrastructure,"[12] this deadline is brought down to 6 hours. An EPsO has to be executed without "undue delay".

f) Enforcement

In order to guarantee the practical effectiveness of the instrument, while taking into account potential reservations and constraints on the side of the service provider or other affected persons, the regulation provides for a set of procedures and tools, some of which are prescribed by the regulation itself, and some of which require intervention on the part of the national legislator. On the one hand, in order to accommodate the interests of the service providers, the regulation provides for instruments of dialogue[13] between law enforcement and service providers in addition to remedies for the latter, the suspects and accused persons as well as for other persons whose data were obtained. On the other hand, in order to guarantee effectiveness of the measures, there are procedures for enforcement which engage authorities in the executing Member State and eventually pecuniary sanctions.

After receiving the order, the service provider would have to perform a check of the order. The draft regulation provides this as a right, but on many occasions the check will instead be a duty because of the contractual relationship with the user or data protection rules. According to the draft, there are three groups of reasons which may create difficulties for the service provider to comply with the order and for which the regulation provides ways of remedying the situation. The objections shall be transmitted to the issuing authority by using a standard form (annexed to the draft regulation).

The first group of reasons concerns the situation when the order is incomplete, contains manifest errors or does not contain sufficient information to execute. In this case, the service provider may ask for clarification. The reasons of the second group arise if the service provider is unable to execute the order because of *force majeure* or *de facto* impossibility, e.g. either because the order does not concern their customer or because the data has been deleted already. If the issuing authority confirms the objection, it shall withdraw the order. The third group of reasons is described as "other". So, for any other reason that the service provider does not provide the requested data within the deadline or does not provide it exhaustively, it shall also send the annex to the issuing authority explaining the reasons for failing to provide the data. The only potential consequence of this action is that the issuing authority shall review the order and, if necessary, set a new deadline. This does not seem to oblige the authority to withdraw the order even if there is good reason to do so.

If the addressee does not comply with the order and the above dialogue procedure does not cause the issuing authority to accept the reasons provided, the issuing authority may transfer the order to the competent authority in the executing Member State. This transforms the procedure into a more traditional mutual recognition process: the enforcing authority should recognise the order, except if there are grounds to oppose, which are enumerated in Art. 14(4) or (5), immunity or privilege under national law, or if its disclosure may impact its fundamental interests such as national security and defence.

So far, the above rules apply to both types of orders (EPdO and EPsO). The draft regulation provides, however, an additional reason for the service provider not to provide information if it comes to the EPdO. This reason is an example of the above-mentioned "other" reasons and refers to an EPdO that "cannot be executed because based on the sole information contained in the [order] it is apparent that it manifestly violates the Charter of Fundamental Rights of the European Union or that it is manifestly abusive." In this case, the service provider must send the respective annex to the enforcement authority in the Member State of the addressee. The latter authority may then seek clarification from the issuing authority, including through Eurojust or the European Judicial Network.

The impact of this rule is problematic. While it seemingly concerns a fundamental question – a significant abuse – it seems only procedural in nature: it requests that another authority be informed, an authority which may be potentially involved if the enforcement is needed. How should this fundamental rights clause be construed? Should it be read as if the violation or abuse is not manifest, it is not a ground to object? Or should it merely be read as saying, that if the violation or abuse is not manifest, the other authority should not receive the annex at this stage? If this provision is read together with the enforcement part, one notices that the executing state authority cannot oppose the execution of the order if it finds that it violates the Charter or that it is abusive, unless the violation/abuse is manifest. It results from this interpretation that, without the fulfilment of this adverbial condition ("manifestly"), the abuse or violation have no relevance and the execution of the EPdO would be obligatory. This is a highly questionable outcome. In addition, the Explanatory Memorandum does not explain how to interpret the word "manifest," which usually means "obvious" or "clearly apparent." Yet, an abuse is an abuse irrespective of whether it is visible *prima facie* or not. If the court in the executing member state reveals its abusiveness, why should it not be allowed to oppose the order just because it was not possible to spot it prima facie?

g) Sanctions and remedies

The draft regulation contains provisions on sanctions (Art. 13) and remedies (Arts. 15–17), although these are relatively restrained, making mostly reference to national law. The Member States are also obliged to put in place provisions on pecuniary sanctions applicable to service providers in the event of infringements of their duties (as described above). While the sanctions do not need to be of a criminal nature, they have to be effective, proportionate and dissuasive. The proposal does not clarify who shall impose a sanction and who should enforce it. It is also not clear whether good reasons to refuse providing information on the part of the service provider, such as a (non-manifest) violation of the Charter or a (non-manifest) abuse of the order (see f) above), may be taken into account in the process of imposing such sanctions.

The draft regulation further contains a chapter entitled "Remedies", which complements the measures described above and grants rights not only to the service providers, but also to suspects and accused persons as well as other persons whose data were obtained. Except for the service providers, the remedies concerning all the other persons are to be provided by national law. Such right to an effective remedy shall be exercised before a court in the issuing state and must offer the possibility to challenge the legality of the measure, including its necessity and proportionality. The issuing authority is also responsible for informing the interested persons about that right (Art. 17). Within this framework these persons should be able to address issues of violation of the Charter or the abuse of the order.

It should also be underlined, that Art. 1(2) of the draft regulation contains the same clause as Art. 1(3) of the Framework Decision on the European Arrest Warrant, which has recently resulted in cases where the execution of the EAW was put under question or refused because of fundamental rights concerns.[14] It cannot be excluded that the clause could result in similar questioning of the orders based on the same or similar concerns.

The service providers' right to remedy is limited to conflicts of laws and affects only the EPdO. This remedy is meant to take into account situations in which the service provider would find itself in a situation where the order obliges it to provide information although the applicable law of a third country prohibits it. According to the Explanatory Memorandum, this approach should also encourage non-EU countries to respect the limitations that the providers falling into the scope of this regulation face, in particular as regards fundamental rights concerns, including data protection.[15] The remedy applies if compliance with the EPdO would result in a conflict with the applicable law of a third country prohibiting disclosure of the data concerned:

- On the grounds that this is necessary to either protect the fundamental rights of the individuals concerned or the fundamental interests of the third country in relation to national security or defence (Art. 15);
- On other grounds (Art. 16).

It is expressly stated that the conflict cannot be based just on the lack of a similar procedure in the third country or on the fact that the data is stored in that country. The service provider shall inform the issuing authority about the existence of the conflict. If the issuing authority intends to uphold the EPdO, it shall request a review by the competent court in the issuing Member State. The court shall verify if the law of the third country applies and if it is so, whether the service provider is prohibited from disclosing the information. The verification can have several consequences:

- If the court finds no relevant conflicts of law, it shall uphold the order;
- If the court finds that there is a conflict because of "other grounds," the court lifting of the order is not mandatory. The court must (only) consider the conflict when evaluating a number of criteria specified in Art. 16(5) that are based on the requirements of data protection, investigation and the addressee's interests;
- If the conflict is grounded in the protection of the fundamental rights of the individuals concerned or of the fundamental interests of the third country in relation to its national security or defence, a central authority of the third state is engaged. This authority shall respond within 15 days (a deadline that may be extended upon request from that authority), whether it objects to the execution of the EPdO. Such an objection obliges the court in the issuing state to lift the order. Lack of response of the authority results in a reminder with a five days deadline and if that brings no reaction, the order shall be upheld. It is worth noticing that the authority in the third state is not obliged to comply with the deadlines. While questions of national security or defence may be a sufficient motivation for the authority to comply with the deadline, the protection of fundamental rights may not in all cases. Then, such an authority in the third country may only be motivated by comity or by the will to protect the service provider because of its connection with the third state.

2. Draft Directive

The draft directive obliges the Member States to set up rules ensuring that service providers offering services in the European Union designate at least one legal representative in the Union empowered to receive and respond to the orders described in the regulation. In order for the regulation to be effective, it is crucial that the name of such representative is

made known, also in view of relatively short deadlines that the regulation imposes for the execution of the orders.

Some Member States have already created such obligations – at the national level – to nominate a service provider's representative. This action is, however, in conflict with the internal market logic: imposing mandatory legal representation within the territory of a Member State is in conflict with the freedom of services within the internal market.[16] Therefore, the directive aims not only to assure the possibility of an effective enforcement of the EPdO and EPsO, but also to avoid the risk that other Member States launch further unilateral initiatives in this regard, creating divergent legal frameworks and further obstacles to the internal market. Hence, the directive is issued on an internal market legal basis, which is explained by its aim. While the problem described affects the service providers that are not established in a Member State in question, it does not exist if they have already been established. As a consequence, and similarly to the draft regulation, the directive does not affect service providers offering services exclusively in the territory of one EU Member State.

The obligation to "designate at least one legal representative in the Union for the receipt of, compliance with and enforcement of decision and order issued by competent authorities of Member States for the purpose of gathering evidence in criminal proceedings" concerns service providers established in the European Union as well as those that are not established in the Union, but offering services in the territory of the Member States concerned (Art. 3 (1) and (2) of the draft Directive). The latter means that such a service provider should have a substantial connection to the Member State. The meaning of substantial connection is the same as for the draft regulation (see above 1c).[17] In order to guarantee the fulfilment of these duties, the Member States should also provide for effective, proportionate and dissuasive sanctions applicable for infringements of these duties and make sure that they are implemented (Art. 5).

III. Next Steps

The Commission's proposal has already been subject to some analysis at the request of the European Parliament[18] as well as by the academic community,[19] civil society[20] and industry.[21] The Council as well as the European Parliament have been discussing the proposal for the regulation. The Council reached an agreement on 7 December 2018 proposing a number of amendments to the Commission's draft.[22] The following are among the most important amendments:

- Including into the scope of application of the regulation that an order may also be issued for the purpose of the execution of custodial sentences or detention orders (with exceptions) (Art. 3);
- Deleting the subsection on orders being manifestly abusive or manifestly violating fundamental rights (Art. 9(5));
- Adding to the provision on sanctions that pecuniary sanctions − of up to 2% of the total worldwide annual turnover of the service provider's preceding financial year − can be imposed (Art. 13);
- Abolishing the differentiation between the two remedies for service providers regarding a conflict of law; according to the new design, the mandatory opinion of the authority of the third country is abolished, and only seeking information from that authority is allowed; it is not obligatory to lift the order, regardless of the conflict of law (Arts. 15 and 16);
- Adding for the EPdOs concerning content data a procedure requesting notification of the authority of the enforcing Member State if there are reasonable grounds to believe that the person whose data is sought is not residing in the territory of the issuing Member State; this procedure, which was one of the major issues discussed in the Council, is meant to safeguard rights stemming from immunities and privileges (new Art. 7a);[23]
- Including the speciality principle providing limitations on the use of electronic evidence other than for the purpose of the proceedings for which it was obtained and its transmission to another Member State, third country or international organisation (new Art. 12b).

Following these conclusions, the Council is ready to start the trilogue negotiations with the European Parliament. Yet, work on the Directive is still ongoing within the Council, which hopes to reach an agreement under the Romanian Presidency.[24] As to the regulation, the Parliament still has to agree on its position, which is being prepared first and foremost by the LIBE Committee. The committee requested two reports[25] and held a public hearing on 27 November 2018, while the designated rapporteur issued a working document, which should help steer further discussion.[26] It is difficult to predict whether the agreement can be achieved before the end of the parliamentary term, given the number of critical voices within the Parliament and also the fair number of reservations on the part of Member States that were expressed during the discussions in the Council.[27]

1 On the *Microsoft Corp. v. United States* known as Microsoft Ireland case, see J. Daskal, "Microsoft Ireland, The CLOUD Act, and International Lawmaking 2.0", (2018) 71 *Stan. L. Rev. Online,* 9. For a description and critical analysis of the cases against Yahoo and Skype in Belgium, see V. Franssen, "The Belgian Internet Investigatory Powers Act – A Model to Pursue at European Level?", (2017) 3 *Eur. Data Prot. L. Rev.,* 534, 538 et seqq.

Dr. Stanislaw Tosza

Assistant Professor at Willem Pompe Institute for Criminal Law and Criminology; Researcher at Utrecht Centre for Regulation and Enforcement in Europe (RENFORCE). Faculty of Law, Economics and Governance, Utrecht University

2 For a complex analysis of legal and technical challenges see K. Ligeti and G. Robinson, "Cross-Border Access to Electronic Evidence: Policy and Legislative Challenges", in: S. Carrera, and V. Mitsilegas (eds.), *Constitutionalising the Security Union: Effectiveness, rule of law and rights in countering terrorism and crime*, 2017, pp. 99–111, as well as K. Ligeti and G. Robinson, "Transnational Enforcement of Production Orders for Electronic Evidence. Beyond Mutual Recognition?", in: R. Kertand A. Lehner (eds.), *Vielfalt des Strafrechts im internationalen Kontext: Festschrift für Frank Höpfel zum 65. Geburtstag*, 2018, pp. 625–644. See also: S. Carrera, G. González Fuster, E. Guild, and V. Mitsilegas, *Access to Electronic Data by Third-Country Law Enforcement Authorities*, Centre for European Policy Studies, Brussels 2015.

3 <https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/council_conclusions_on_improving_criminal_justice_in_cyberspace_en.pdf> accessed on 29.01.2019.

4 The Commission issued in 2017 a non-paper: "Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward" and conducted public consultation. Furthermore, it issued an impact assessment. All documents can be found here: <http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-cross-border-access-to-e-evidence> accessed 21 December 2018. For the legislative proposals themselves, see COM (2018) 225 final [draft Regulation] and COM (2018) 226 final (draft Directive). See also T. Wahl, "Commission Proposes Legislative Framework for E-Evidence", *eucrim* 1/2018, 35–36.

5 The abbreviations proposed by the Regulation are rather unfortunate, i.e. "EPOC" for the production order and "EPOC-PR" for the preservation order. This is confusing because both words – production and preservation – start with the letters "PR". The author suggests and uses the abbreviations "EPdO" and "EPsO". These abbreviations are much easier for an immediate recognition which instrument is being referred to. They would also be much easier for the respective certificates, hereinafter: "EPdOC" and "EPsOC".

6 If not stated otherwise, references to Articles in the following refer to the draft regulation.

7 Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final, Explanatory Memorandum, pp. 14–15. For an alternative proposal regarding a new categorization of data in the context of fundamental rights interferences, see the article of C. Warken in this issue.

8 V. Franssen, "The European Commission's E-Evidence Proposal: Toward an EU-Wide Obligation for Service Providers to Cooperate with Law Enforcement?", *European Law Blog* (12 October 2018), <https://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/> accessed on 29.01.2019.

9 Explanatory Memorandum, p. 14.

10 Explanatory Memorandum, p. 15.

11 Again, the regulation uses confusing abbreviations: EPOC and EPOC-PR. This article proposes to use EPdOC and EPsOC instead (see note 5).

12 Art. 2(15) of the draft regulation. Critical infrastructure is defined by reference to the Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection – Art. 2(a).

13 As the Explanatory Memorandum puts it: Explanatory Memorandum, p. 19.

14 ECJ, 5 April 2016, Joined Cases C404/15 and C659/15 PPU, *Aranyosi and Căldăraru*; ECJ, 25 July 2018, Case C-216/18 PPU, *LM*.

15 Explanatory Memorandum, p. 21.

16 Recital 3 of the Directive.

17 Recital 13 of the Directive.

18 See E. Sellier and A. Weyembergh *Criminal procedural laws across the European Union – A comparative analysis of selected main differences and the impact they have over the development of EU legislation*". The study is of a more general nature, but touches upon the e-evidence proposals well. It can be retrieved from the Internet via the following link: <http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITEES/LIBE/DV/2018/10-10/IPOL_STU2018604977_EN.pdf> accessed on 29.01.2019. See further M. Böse, *An assessment of the Commission's proposals on electronic evidence*: <http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604989/IPOL_STU(2018)604989_EN.pdf> accessed on 29.01.2019.

19 Inter alia: V. Franssen, *op. cit.* (n. 8); G. Robinson, "The European Commission's e-Evidence Proposals", (2018) 3 *European Data Protection Law Review*, 347; T. Christakis, "E-Evidence in the EU Council: The Key Issue of When One Member State Can Review the Requests from Another", posted on October 1, 2018 at the *Cross Border Data Forum* <https://www.crossborderdataforum.org/e-evidence-in-the-eu-council-the-key-issue-of-when-one-member-state-can-review-the-requests-from-another/> accessed on 29.01.2019.

20 <https://cdt.org/insight/cdt-recommendations-for-improving-the-european-commissions-e-evidence-proposals/> accessed on 29.01.2019.

21 <http://www.euroispa.org/e-evidence-euroispa-adopts-position-paper/> accessed on 29.01.2019; <https://blogs.microsoft.com/on-the-issues/2018/09/11/a-call-for-principle-based-international-agreements-to-govern-law-enforcement-access-to-data/> accessed on 29.01.2019.

22 Council Interinstitutional File: 2018/0108(COD).

23 The future of this provision will be particularly interesting because a large number of Member States made reservations to this provision. See also T. Christakis "'Big Divergence Of Opinions' On E-Evidence In The EU Council: A Proposal In Order To Disentangle The Notification Knot", posted on 22 October 2018, <https://www.crossborderdataforum.org/big-divergence-of-opinions-on-e-evidence-in-the-eu-council-a-proposal-in-order-to-disentangle-the-notification-knot/> accessed on 29.01.2019.

24 Council of the European Union, "Regulation on cross border access to e-evidence: Council agrees its position", *Press Release of 7 December 2018.*

25 See note 18.

26 <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-631.925+02+DOC+PDF+V0//EN&language=EN> accessed on 29.01.2019.

27 S. Stolton, "Council makes half-hearted agreement on e-Evidence", *euractiv* (7 December2018), <https://www.euractiv.com/section/digital/news/council-makes-half-hearted-agreement-on-e-evidence/> accessed on 29.01.2019.