CROSS-BORDER GATHERING OF ELECTRONIC EVIDENCE: MUTUAL LEGAL ASSISTANCE, ITS SHORTCOMINGS AND REMEDIES[1]

Stanislaw TOSZA
Assistant Professor at Willem Pompe Institute
for Criminal Law and Criminology
Researcher at Utrecht Centre for Regulation
and Enforcement in Europe (RENFORCE)

A large number of criminal offences, not only cybercrime, is currently committed in a way that leaves digital traces which 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 possession of Internet service providers (ISPs), 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.

The current MLA framework presents various shortcomings, in particular, the length of the MLA procedure combined with the fast pace of activities by means of information and communication technology and the possibility of the loss of data. In view of the deficiencies of this mechanism, law enforcement authorities have a tendency to circumvent MLA rules in practice.[2] For instance, they request data directly from the ISPs, wherever they have their headquarters or office, or conduct digital searches in computers systems located abroad (e.g. by means of Trojan horses).[3] Both approaches have significant legal and practical drawbacks. In particular, the first one generated already significant jurisprudence (e.g. the Belgian *Yahoo!* and *Skype* cases and the US *Microsoft Ireland* case) demonstrating the diversity in potential approaches, which

1 The text contains few parts that have been already published as "The European Commission's Proposal on Cross-Border Access to E-Evidence. Overview and Critical Remarks" in eucrim 4/2018, pp. 212-219, which contains a more detailed analysis of the Commission's proposal.

2 S. Carrera, G. González Fuster, E. Guild, V. Mitsilegas, *Access to Electronic Data by Third-Country Law Enforcement Authorities*, Centre for European Policy Studies, Brussels 2015.

3 J. Daskal, *The Un-Territoriality of Data*, 125 Yale L. Rev. 326 (2015).

results in legal uncertainty for ISPs and which affects the rights of persons concerned by requests for information. It seems a save assumption that criminal procedure will become more and more dependent on digital evidence in the coming years, hence the need for a clear legal framework regarding its cross-border exchange.

The first aim of this paper is to show the basic parameters of the MLA regime and its shortcomings that currently cause disaffection among the policy-makers and academics alike. Furthermore, it will present possible solutions to today's problems, in particular focusing on two initiatives undertaken on both sides of the Atlantic, which should offer a different system of acquisition of data based on direct requests issued by law enforcement authorities in one country to service providers in another, thereby circumventing the intervention of competent authorities in the country of the service provider in question.

Before this contribution embarks on its analysis, it is important for the reader to understand the complexity of the problems stemming from two main sources: legal and technological. As to the legal difficulties, it touches upon several domains of law, including: criminal procedure, where the power of law enforcement to ask for data is naturally embedded; international law, which sets the territorial limits for the prosecutorial power[4]; telecommunication law providing for obligations of service providers which fall into its scope; and finally data protection, which sets the data management framework for service providers.

The technical difficulties are also numerous. The classic approach to cross-border exchange of data presumes territoriality, which is linked with the location of data. However, that concept seems outdated in view of the technical advancements, loss of localisation (with each time larger amount of data being stored in the cloud, hence without a concrete long term location), or even lack of data as such (e.g. part of Skype services use technology where data is not stored on a server, but transferred directly peer-to-peer from one computer to another) and the limits of enforcement (e.g. the Police would have real difficulties to examine a data centre in order to find data stored there without cooperation of the service provider given the limited resources of law enforcement and the amount of data stored there).

4 On this point see in particular the analysis: Ulich Sieber, Carl-Wendelin Neubert, Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty. In: Lachenmann, F., Röder, T. J., Wolfrum, R., Max Planck Foundation for International Peace and the Rule of Law (eds.), Max Planck Yearbook of United Nations Law, vol. 20 (2016). Brill, Nijhoff, Leiden 2017, pp. 241-321.

I. Shortcomings of mutual legal assistance

MLA is the default legal framework that law enforcement must use in order to request data in a compelling way in a situation that it cannot consider domestic, so basically where the data is held abroad or the service provider is not present in one way or another in the country in question, which would result in being subject to obligations stemming from the law of that country. Within the European Union law enforcement may resort in principle to the European Investigation Order, which will be discussed more in details below. However, if the data has to be requested from a non-EU country, MLA has to be used. This method of cooperation is of high importance in the digital context, as the most important providers, such as Google (that also owns YouTube), Facebook (owner of WhatsApp and Instagram), Microsoft (owner of Skype) are American.

The US and the European Union signed an MLA Agreement on 25 June 2003,[5] which entered into force on 1 February 2010. Yet this agreement concerns only some aspects of cooperation and does not contain a legal basis for requesting digital evidence. The latter has to be found in the bilateral agreement between each of the EU Member States and the US. The legal basis of mutual legal assistance between Belgium and the United States is the Treaty of 28 January 1988 between the United States of America and Belgium, which was further amended with an Instrument of 16 December 2004 that included provisions stemming from the EU-US Agreement.[6] Article 6 of the Treaty provides for the legal basis for transmitting production orders and Articles 15-18 provide for rules on procedure.

The procedure is similar as in other treaties of mutual legal assistance and requires that the authority seeking the data sends a request to its domestic Central Authority, the Minister of Justice or his/her representative in case of Belgium, who then transmits it to the US Attorney General. According to Article 16 (2) of the Belgium-US Treaty "[r]equests shall be executed according to the domestic laws and procedures of the Requested State". In case of requests made by Belgian authorities to the US, this means that US will apply. In consequence, the representatives of the Attorney General prosecutor has to ask the court for an authorisation

5 Agreement Between the United States of America and the European Union signed at Washington 25 June 2003, accessible at: https://www.state.gov/documents/organization/180815.pdf.

6 Treaty of January 28, 1988 between the United States of America and Belgium, and the Instrument Amending the latter signed at Brussels on 16 December 2004, accessible at: https://www.state.gov/documents/organization/188253.pdf.

and in particular prove that the domestic standard of probable cause has been fulfilled.[7] If the competent judge is not satisfied with the supplied evidence to meet this threshold, the Attorney General's representatives have to ask the Belgian authorities to supplement information and reapply for the data (which in the meantime may be gone or have been anonymised).[8]

Already from this description the reader may deduct the major shortcoming of this system, which is its length.[9] On average this procedure takes 10 months.[10] The second major difficulty is constituted by the US evidentiary standard of probable cause (that the data is evidence of a crime).[11] This requirement stemming from the 4th Amendment to the US Constitution is a subject of an extensive body of jurisprudence, but remains still vague in practice.[12] As it is not familiar to European judges, it is not a rare occurrence that they have difficulties to meet that standard in their application, which considerably delays the procedure.[13] This problem has been already recognised by the European Commission, which committed considerable funds for training of European judges in that respect.[14]

Further to the length and probable cause requirement (affecting also the former), the MLA framework presents further shortcomings, as was pointed out in the Commission's Non-Paper, which summarises the Commission's evaluation of the issue among the EU Member States. In particular, it is considered to be too complex and too resource intensive, given the cumbersome procedure described above, engaging various authorities of both countries. They are thus disproportionate to cases that

7 Tiffany Lin, Mailyn Fidler, Cross-Border Data Access Reform: A Primer on the Proposed U.S.-U.K. Agreement, September 2017, p. 2.

8 See also on this procedure more in general Jennifer Daskal, Unpacking the CLOUD Act, eucrim 4/2018, p. 222.

9 See also a good analysis of the shortcoming of this procedure by Gail Kent, "The Mutual Legal Assistance Problem Explained", published on 23 February 2015 at http://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained.

10 Richard A. Clarke *et al.*, "Liberty and Security in a Changing World. Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies (2013), accessible at https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf, p. 227.

11 Statement of Jennifer Daskal to the Committee on the Judiciary Subcommittee on Crime and Terrorism United States Senate. Hearing on Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights, May 10, 2017, p. 3.

12 Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment, October 2017 Update, Thomson Reuters, § 3.1 ff.

13 Technical Document: Measures to improve cross-border access to electronic evidence for criminal investigations following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_technical_document_electronic_evidence_en.pdf, pp. 8-9.

14 EU Commission Non-paper: Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward, accessible at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf, p. 3.

are purely domestic, with perpetrators, victims and facts being limited to one country. The complexity of the MLA procedure also results also in incorrect or inadequate requests.[15]

II. Existing alternatives

Law enforcement is trying to find practical and legal solutions to the problems describes above. Among the most important ones is voluntary cooperation of service providers and unilateral direct access to data.[16] These will be analysed below. Finally, another solution, which might help to acquire data, but was not designed for this purpose *per se*, is the already-mentioned European Investigation Order. Its applicability to the issues under examination in this article will be briefly discussed too in this section.

Before proceeding with this analysis, it is worth mentioning that not only tendencies to look for new solutions are present, but also tendencies to stick to mutual legal assistance, despite its impracticality, and to a territorial approach to data, despite its antiquatedness (*supra*). This approach was most notoriously presented in the so-called Microsoft Ireland case where the US government sought, by means of national law, data from Microsoft and the latter refused because the data was stored at the data centre in Dublin. Because of the latter fact Microsoft required an MLA sent to Ireland. The Court of Appeal gave reason to Microsoft,[17] and the case was taken by the Supreme Court, which even held a hearing on the case. The case was, however, mooted it in view of the legislative changes that occurred in the meantime.

The key question of the case was whether there was exterritorial application of the US law (i.e. of the Stored Communications Act) or whether the situation was domestic in terms of the application of the law.[18] The

[15] EU Commission, Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace, http://data.consilium.europa.eu/doc/document/ST-15072-2016-REV-1/en/pdf, p. 5.

[16] Unilateral (or unmediated) access is characterised by "*the lack of consent by the requested stated and the non-intervention by an independent authority* in the requested EU state validating the lawfulness of accessing and processing data" (S. Carrera, G. González Fuster, E. Guild, V. Mitsilegas, *Access to Electronic Data by Third-Country Law Enforcement Authorities*, Centre for European Policy Studies, Brussels 2015, 9, emphasis in the original) ; lack of consent is the result of consent not being sought for and not a negative decision.

[17] The Petition for a Writ of Certiorari and the decision of the Court of Appeals for the Second Circuit are accessible at: https://www.scotusblog.com/wp-content/uploads/2017/07/17-2-petition.pdf.

[18] There was agreement that exterritorial application of the Stored Communications Act was excluded.

former was argued by Microsoft based on the place where the data was stored, so applying territoriality; i.e. since the data was held abroad, the request made by the US government was reaching beyond the US borders. The US government focused on the ability of Microsoft to access and control the data from the United States arguing that the situation is domestic in the sense that Microsoft was able to access and control the data from the US so any seizure or production would be done from the US, hence rendering the case domestic, and not extraterritorial. Given the enactment of the CLOUD Act, in particular its Part I dealing with US law enforcement reach regarding data held by US providers outside of the US (see below), the solution to this dilemma was solved in the legislative rather than the judicial way. The Act sided with the position of the government. In view of that, there was no need for the Supreme Court to decide on the case.[19]

Section 1. *Voluntary (Direct) Cooperation*

A solution that has been applied in practice is direct cooperation between law enforcement and the companies.[20] It consists in authorities sending their request directly to the service providers abroad and relying, in principle,[21] on their good will to provide data for investigation or prosecution purposes.

In particular, US service providers are allowed to provide foreign law enforcement authority with non-content data on a voluntary basis according to the Electronic Communications and Privacy Act 1986, and differently than regarding the content of communications which due to the so called "blocking provision" are forbidden to be furnished to foreign law enforcement by the US service providers.[22] In consequence, data requests can be sent and answered to without resorting to the MLA procedure and thus without the involvement of the US judicial authorities. These types of constraints do not concern only the US providers. In the case discussed below, Skype (headquartered in Luxembourg) was

19 Jennifer Daskal, Unpacking the CLOUD Act, eucrim 4/2018, p. 221.

20 EU Commission Non-paper: Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward pp. 1, 3-4; EU Commission, Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace, p. 4.

21 According to the study of the EU Commission 7 Member States consider such requests to be mandatory. EU Commission, Non-paper: Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace, p. 4.

22 *Id.*, p. 6; 18 U.S.C., § 2702.

prevented from producing data requested by the Belgian authorities by the Luxembourgish law.

While this cooperation gives more flexibility and allows circumventing the troubles of the MLA regime, it raises doubts as to the protection of the rights of individuals concerned for lack of clear legal framework. The procedure lacks transparency and accountability, hence such an approach is questionable in the rule of law system. It has also clear limitations as there is no remedy for law enforcement in case of lack of will to cooperate on the side of the ISP. Other problems also hinder the practical application of this method, such as lack of common rules as to the contact points to receive requests from law enforcement, which result in these contact points being established at national, regional or global level, or not being established at all.[23] On the side of the service providers, the difficulty consists in assessing the authenticity of requests and their legality.[24] Finally, there may be problems with the admissibility of evidence gathered in that way.[25]

In conclusion, for the reasons above and given the limitations in its application, voluntary cooperation cannot become a general solution to the problem of cross-border transfer of evidence.

Section 2. *Unilateral access*

The limited practical applicability of voluntary cooperation was demonstrated by the Belgian case of Yahoo !, which can also be seen as the opposite of the approach adopted by the courts in the Microsoft Ireland case cited above. Yahoo refused to provide non-content data (subscriber data, and also dynamic IP addresses, the date and the time of the accounts' creation)[26] requested by a Belgian prosecutor (in a purely domestic case) claiming that being an American company, it is prevented from doing so by American law and requested the Belgian authorities to use the MLA procedure. Instead of resorting to this procedure, the Belgian prosecutor decided to prosecute the company for non-cooperation, which resulted in a judicial saga. One of the main legal arguments concerned whether Yahoo can be considered a Belgian company for

[23] *Id.*, p. 8.
[24] *Id.*, p. 9.
[25] *Id.*, pp. 5, 10.
[26] Vanessa Franssen, The Belgian Internet Investigatory Powers Act – A Model to Pursue at European Level, 3 Eur. Data Prot. L. Rev. 534 (2017), p. 538.

the sake of obligations stemming from the Code of Criminal Procedure (in particular Article 46*bis*). While Yahoo pointed to it not having any physical presence in the country (i.e. lack of headquarters or any infrastructure), the prosecution focused on its virtual presence resulting from targeting its services to local customers (e.g. use of local languages, local advertisement).[27] The courts, including the Supreme Court, sided with the approach championed by the public prosecution.[28]

Another landmark case which went into the same direction concerned Skype. This service is headquartered in Luxembourg and also refused to provide requested data (traffic and location data, but more importantly the content of live communication), including communication content, citing it not having any physical presence in Belgium. This refusal resulted in a criminal fine for non-cooperation for Skype upheld at the appeal level.[29] The case not only confirmed the approach established in the Yahoo ! case. Skype was an intra-EU case and also concerned the content of communication.

Furthermore, the Belgian legislator adopted the approach presented by the law enforcement side in both cases concerning the extensive personal scope of duty to cooperate by including it in three provision of the Code of Criminal Procedure imposing cooperation duties on service providers (Arts. 46*bis*, 88*bis* 90*quater*).[30]

There are two main problems with this solution. Firstly, exterritorial application of domestic law is questionable under international law standards. Furthermore, while one may consider such a solution justified in purely domestic cases (as were Yahoo ! and Skype), also taking into account the protection given by criminal procedure domestically, nothing would preclude the application of this approach to situations where the local link would be less obvious.[31] The result might also be less than satisfactory, if the approach would be applied by countries with poor human rights' protection standard. Secondly, the enforcement of such a solution would become a battle of effectiveness between law enforcement of different countries, which is hardly a desired solution. Thirdly, and as a consequence of the two previous arguments, such an approach is very cumbersome for the business community, as it creates uncertainty as to applicable rules and conflicting obligations.

27 *Id.*, pp. 538 et s.
28 Cass 1 December 2015, No P.13.2082.N.
29 Vanessa Franssen, The Belgian Internet Investigatory Powers Act – A Model to Pursue at European Level, 3 Eur. Data Prot. L. Rev. 534 (2017), p. 539.
30 *Id.*, pp. 539-540.
31 *Id.*, p. 539.

Section 3. *European Investigation Order*

The (relatively) new European Investigation Order (EIO) is a crucial piece of legislation aimed at facilitating cooperation between the judicial authorities of the EU Member States. It could also serve to facilitate obtaining data held by companies in another Member State than the place where the investigation is taking place. However, the EIO was not designed with gathering of digital evidence in mind. There is no mention of it as such, with measures directed either at the collection of the "real world evidence" or at banking of financial data, or at "life" interception of communication.

This aspect is mainly visible in the fact that the EIO does not take into account the direct cooperation between law enforcement and service providers as well as its relatively long deadlines. As to the first argument, the EIO is based on mutual recognition and works in practice in the same way as other mutual recognition instruments of the EU, like the European Arrest Warrant. The procedure still requires contact between judicial authorities and only the executing State's competent authority may order the Internet service provider to provide data.

Its deadlines might also be considered too slow for the demands of the digital world, particularly in view of the volatility of data. The time limit of 90 days for executing the measure is extremely lengthy, and it follows an already long period of 30 days for deciding whether to recognise the EIO (Article 12 (3) and (4) EIO). An emergency procedure is not foreseen. The issuing authority may ask for a shorter deadline and the executing authority "shall take as full account as possible of this requirement" (Article 12 (2) EIO).

III. The Commission E-Evidence Initiative

The shortcomings of the existing legal framework and the urgent need to address the problem of cross-border gathering of electronic evidence has been acknowledged at the European Union level. In its Conclusions of 9 June 2016, the Council requested the Commission to develop a legal framework that would allow law enforcement to obtain relevant data.[32] This request lead to the proposal of the Commission published on 17 April 2018.[33]

[32] 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.

[33] The Commission issued in 2017 a non-paper (mentioned already above): "Improving cross-border access to electronic evidence: Findings from the expert process and suggested way forward" and conducted public consultation as well as issued an impact assessment. These documents may be found here: http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-cross-border-access-to-e-evidence.

The Commission's proposal is composed of two instruments: a Regulation and a Directive. The Regulation, if adopted, would create two new instruments: European Production Order (henceforth: EPdO, this article suggests a change in the abbreviation from the Commission's proposal) and European Preservation Order (henceforth EPsO, also a change is suggested).[34]

An EPdO 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 produce electronic evidence" (Article 2 (1) of the draft Regulation). 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" (Article 2 (2) of the draft Regulation). It is interesting to note than an EPsO may result not only in an EPdO, but also for instance in a mutual legal assistance request or a European Investigation Order (Article 6 (2) of the draft Regulation).

What is the crucial characteristic of this proposal is that the order 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 at the level of 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 Directive obliges the Member State 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.

What is also noteworthy is the choice of the legal basis and of the instrument. The Directive has an internal market legal basis (see analysis below), and the Regulation is issued based on Article 82 (1) TFEU.

Given the importance of this initiative, its most important aspects will be presented here in a more detailed way.[35]

[34] The abbreviations proposed by the Regulation are rather unfortunate. EPOC for the production order and EPOC-PR for the preservation order. Since both words – production and preservation – start with the letters "PR" the risk of confusion is high. In view of the author, the abbreviation EPdO and EPsO would be much easier for an immediate recognition which instrument is being referred to, and also in the spoken language. It would also be much easier for the respective certificates: EPdOC and EPsOC.

[35] This exposé presents the proposal according to the original EU Commission's Proposal. The discussions at the Council led to the adoption on 4 December 2018 of the General Approach that proposes some change, some of great significance, although it does not change the overall architecture of the proposal as described here (Interinstitutional File: 2018/0108(COD), available at: https://data.consilium.europa.eu/doc/document/ST-15020-2018-COR-1/en/pdf). The adoption of the general approach opens the way for the trialogue as far as the Council is concerned and the burden is now on the side of the Parliament that

Section 1. *The draft Regulation*

According to the proposal for the Regulation, EPdO and the EPsO have the same object: they oblige the service provider to respectively produce or preserve electronic evidence. The latter term is explained in Article 2 (6) of the draft Regulation. There are three elements to this definition. 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 data that is already in possession of the service provider and not any data obtained in the future, thus excluding any future surveillance. Thirdly, the term evidence is not defined as such, but by enumerating and defining four types of data of which that evidence might consist: subscriber data, access data, transactional data and content data.

The four categories of data are in turn defined in the draft Regulation in Articles 2 (7) – (10). The spectrum includes content and non-content data, with the latter being divided into three categories: subscriber data, access data and 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 transaction and content data, where the intrusiveness is more significant. The differentiation affects, in particular, the possibility of using the order (which for the second group is limited only to some categories of offences, but open to all offences as far as the first group is concerned) and the role of the prosecutor (excluded for the second category). According to the Explanatory Memorandum to the proposal, the differentiation between the two categories is made according to the philosophy that data related only to the identification of the user is less intrusive and can be made more accessible and where more of the content of his/her activity is involved, that should be more protected.[36] The Explanatory Memorandum considers that the starting point of an investigation is often the subscriber or access data in order to reveal the identity of the suspect, before data about the content is sought.[37] However,

is working to adopt its position, which will open the way for the trilogue negotiations. For more details on the changes proposed by the Council, see: Theodore Christakis, *E-Evidence in a Nutshell: Developments in 2018, Relations with the Cloud Act and the Bumpy Road Ahead*. posted on 14 January 2019 at: https://www.crossborderdataforum.org/e-evidence-in-a-nutshell-developments-in-2018-relations-with-the-cloud-act-and-the-bumpy-road-ahead/.

36 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.

37 *Id.*, p. 14.

even identification data can be extremely revealing, in particular access data.

Three categories of authorities can be singled out as to their entitlement to issue EPdO or EPsO (Article 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 compose this group. The second group is composed of prosecutors whose authority is limited to what the draft considers to be less sensitive measures (Recital 30 of the Preamble). The prosecutors may issue the EPsO for any type of data, but the EPdO only for subscriber and access data. 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". The order issued by such an authority will need to be examined for its conformity with the conditions set out for the validity of the orders. The authorities entitled to validate the order are the same two groups as for issuing the order and according to the same areas of competences (i.e. the prosecutor's competence is limited to the less intrusive types of data).

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 Article 2 (3), can be:

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

These categories are explained in more details in the Explanatory 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.[38] As to the last category, it makes reference to the providers of internet infrastructure services who hold data that may be of high relevance for identifying the persons of interest.[39]

[38] 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 January 2019.

[39] 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, p. 14.

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 (Article 2 (4)) and its Explanatory Memorandum.[40] 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.

According to the proposal the deadlines for the execution of the orders are much shorter than for instance for the EIO, namely 10 days since the reception of the order in normal circumstances, and 6 hours in urgent cases for the EPdOs (Article 9). The EPsOs have to be executed without undue delay (Article 10).

The draft Regulation contains conditions of issuing both types of orders, including a proportionality and necessity check. In case of subscriber or access data, proceedings for any criminal offence allow the competent authorities to issue an EPdO. However, the issuing of the EPdO for transactional or content data is limited to two groups of offences. The first one depends on 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 group is composed of offences listed by the draft, which have been subject to harmonisation and usually imply e-evidence (e.g. terrorism, attacks against information systems). The draft Regulation also contains provisions aiming at guaranteeing effective enforcement (Articles 13-14), remedies for service providers and persons concerned (Articles 15-17), in particular detailed provisions regarding conflicts of legal obligations with third countries (Article 15-16).

Section 2. *The 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

[40] *Id.*, p. 15.

Regulation to be effective, it is crucial that such representative is known, in view also of relatively short deadlines that the Regulation imposes for the execution of the orders.

As the problem had been already identified by some Member States (e.g. Germany),[41] they created such obligations at the national level. This is, however, in conflict with the internal market logic: imposing mandatory legal representation within a territory of a Member State is in conflict with the freedom of services within the internal market.[42] So not only the Directive should assure the possibility of effective enforcement of the European Production and Preservation Orders, but also avoid the risk that other Member States take further unilateral initiatives in that regard creating divergent legal framework and further obstacles to the internal market.[43] That is the reason why the Directive is issued on an internal market legal basis. This problem affects the service providers which are not established in the issuing State. Hence, and similarly to the draft Regulation, the draft Directive does not affect service providers offering services exclusively on the territory of one 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 on its territory (Article 3 (1) and (2) of the draft Directive). The latter means that such a service provider should have a substantial connection to the Union.[44]

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 (Article 5).

In sum, the twin proposal aims at offering a comprehensive system that should resolve the problem of cross-border access to digital evidence at the European Union level. It does not, as it cannot, solve the problem regarding acquiring data from the US. The changes in that regard will be

41 Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM/2018/226 final, Explanatory Notes, pp. 1-2.

42 Preamble of the Directive, Recital 3.

43 Directive, Explanatory Notes, pp. 1-3.

44 Directive, Explanatory Notes, p. 8. The meaning of substantial connection is the same as for the draft Regulation, see Preamble of the Directive, Recital 13.

discussed in the next section. One can, however, assume that if the EU provides for a solid legal framework, it strengthens its negotiation position with the US government. The importance of that position should be clear to the reader by the end of next section.

IV. The CLOUD Act

As it was mentioned above, one of the crucial factors regarding the gathering digital evidence by law enforcement in the EU Member States is the fact that the most important service providers are US companies. They may provide non-content data to foreign law enforcement agencies but are limited as regards the content data by the Electronic Communications and Privacy Act 1986. This may result in conflicting obligations if the companies are compelled to provide data in another country, as well as in an unnecessary burden on the US officials who need to deal with MLA requests in cases that have nothing to do with US citizens or residents.

In view of the above, in March 2018 the US Congress passed and the President signed the Clarifying Lawful Overseas Use of Data Act (the so-called CLOUD Act).[45] Even if the history of the Act becoming law may suggest that it was rushed through the legislative procedure, the content of the Act is the result of a long discussion among policy-makers, industry, NGOs and academics.[46] While criticised by civil society community for giving too much power to the government, it has been considered an important step forward in walking away from the cumbersome MLA system, while guaranteeing sufficient protection for the persons concerned.[47]

This Act amends the US law lifting the blocking provision and thus allowing the US companies to provide non-US law enforcement with content data, but at several conditions. Firstly, the data may concern only non-US citizens not residing in the US. Secondly, an executive agreement

[45] See in particular the publications of Jennifer Daskal and Peter Swire cited below and other published at: https://www.lawfareblog.com and https://www.justsecurity.org, Theodore Christakis, E-Evidence In a Nutshell: Developments in 2018, Relations with the Cloud Act and the Bumpy Road Ahead published at https://www.crossborderdataforum.org/e-evidence-in-a-nutshell-developments-in-2018-relations-with-the-cloud-act-and-the-bumpy-road-ahead/ on 14 January 2019, Secil Bilgic, Something Old, Something New, And Something Moot: The Privacy Crisis under the CLOUD Act, Harvard Journal of Law & Technology Volume 32, Number 1 Fall 2018.

[46] Jennifer Daskal, Unpacking the CLOUD Act, eucrim 4/2018, p. 220.

[47] Jennifer Daskal, Peter Swire, Why the CLOUD Act is Good for Privacy and Human Rights, published at: https://www.lawfareblog.com/why-cloud-act-good-privacy-and-human-rights on 14 March 2018.

is necessary between the US and that country. The agreement would be concluded based on the assessment of a set of criteria, which the CLOUD Act enumerates concerning this country's standard of the rule of law and the protection of privacy.[48] This agreement would necessarily be reciprocal, so the service providers of that country must also be allowed to respond positively to analogous requests from US law enforcement.[49]

While at the moment of writing it has been almost a year since the adoption of the Act, there is no information as to an agreement of this kind being signed. An agreement has been in negotiations with the United Kingdom (which started long before the adoption of the CLOUD Act), yet the content of a draft is not public and the date when it could potentially be signed is unknown.[50]

One of the crucial questions from the perspective of Europe, is whether the agreements will be negotiated with individual EU Member States or with the European Union as a whole. The positive effect of the latter solution is hard to overestimate as it would avoid potential discrepancies between agreements within the Area of Freedom, Security and Justice and a common playing field for all actors within this area, including certainty for the service providers.[51] The hopes for this solution has been just raised, as the Commission has just issued a recommendation for a Council Decision to open the negotiations in that direction.[52]

Conclusions

It is not too bold a prediction to say that the importance of digital evidence for criminal investigation and prosecution will only be growing in the coming years. In result, the need to provide law enforcement with effective access to it will be pertinent and increasingly urgent. While the MLA regime with its shortcoming seems too much of a cumbersome

48 See Jennifer Daskal, Microsoft Ireland, *The CLOUD Act, and International Lawmaking 2.0*, 71 Stan. L. Rev. Online 9 (2018).

49 Jennifer Daskal, Unpacking the CLOUD Act, eucrim 4/2018, p. 223.

50 Peter Swire, Justin Hemmings, Recommendations for the Potential U.S.-U.K. Executive Agreement Under the Cloud Act, published at: https://www.lawfareblog.com/recommendations-potential-us-uk-executive-agreement-under-cloud-act on 13 September 2018.

51 See also US Authors discussing this: Jennifer Daskal, Peter Swire, A Possible EU-US Agreement on Law Enforcement Access to Data?, LAWFARE, published on 21 May 2018 at https://www.lawfareblog.com/possible-eu-us-agreement-law-enforcement-access-data.

52 Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, 5 February 2019, COM(2019) 70 final.

option, the panorama of alternatives does not offer yet an optimal solution. One should not forget that the problem concerns also other jurisdictions and solutions are being sought also on the global level.[53]

In particular, it remains to be seen what becomes of the two most important initiatives – the CLOUD Act and the EU E-Evidence Initiative –. As to the former, although it has been already enacted, it is not yet functioning in practice as no bilateral agreement has been signed yet. Only the future will tell how the CLOUD Act will function in practice as to its international aspect. Contrary to the US legislation, the EU initiative is just a proposal that still needs to go through the whole EU legislative procedure and if accepted requires as to the Directive to be implemented by the Member States. Even the Regulation will need some national legislation to be enacted. Only then it will be possible to assess it as a model for cooperation between law enforcement and the service providers, both from the perspective of practical functionality and the safeguarding of the rights of affected persons.

The way in which these two initiatives develop in practice will also shape the future of cross-border gathering of digital evidence.

February 2019

[53] Interested reader may for instance look at the initiatives under the umbrella of the Internet & Jurisdiction Policy Network (https://www.internetjurisdiction.net).