

GATHERING E-EVIDENCE IN CROSS-BORDER CASES: RECENT DEVELOPMENTS IN EU LAW

Aleksandar Chavleski

Faculty of Law, FON University, Skopje, Republic of N. Macedonia, aleksandar_chavleski@yahoo.com

Goce Galev

Faculty of Law, FON University, Skopje, Republic of N. Macedonia, gocegalev@gmail.com

Abstract: With the fast development of the digital technology, the need for efficient gathering of digital evidence in criminal cases has risen exponentially. Often, the digital data is stored on servers located abroad, so national authorities cannot obtain them without seeking legal aid from their counterparts in foreign country/territory. This cooperation often doesn't work seamlessly not only from legal, but from factual reasons as well. Here series of questions regarding national sovereignty, jurisdiction and international law are intertwined. In order to achieve sufficient speed in processing such requests, national authorities tried to bypass their counterparts in foreign countries and communicated directly with the service provider. These investigations are time-sensitive in order both to secure the evidence and its integrity. In order to adequately address these concerns, in June 2016 the Council of EU called the Commission to prepare an e-evidence package, which was eventually presented in April 2018. The aim of this article will be to give a critical overview of the proposed package mainly via its key component – the draft Regulation.

Keywords: European Union, digital evidence, criminal proceedings

1. INTRODUCTION

In today's world, almost all crimes contain some form of digital evidence. Moreover, digital data is practically inevitable almost in any criminal or civil case because of their volume and geographical spread.⁶³ In transnational crimes, the fast and secure exchange of digital evidence has become increasingly important. Even in *prima facie* pure domestic criminal cases where the victim is domestic, relevant electronic evidence may be stored by a service provider in a cloud arrangement in another state.^{64 65}

For instance, in most of the terrorist attacks carried out on EU soil in the recent years, the terrorists/conspirators communicated via various online platforms, so the national authorities must adapt to the new technologies and use adequate tools to detect, preserve and obtain such digital evidence. The success of cross-border investigations aimed at obtaining e-evidence in foreign jurisdictions largely depends on contemporary legal and procedural frameworks and functional legal instruments for international cooperation.⁶⁶ However, the present cooperation is based mostly on a patchwork of international agreements on mutual legal assistance, and to a large extent non-harmonized legislation on these issues among the states. Often the instruments for Mutual legal assistance do not work because applying them could infringe national law.⁶⁷ Some countries even resorted to create national cyberspace, passed laws that every company that operates on the Internet to have registered offices on their territory and keep the data

⁶³ See in more detail: Mason, S., "Some International Developments in Electronic Evidence", in: Kin, L. (ed.) *International Conference on Electronic Litigation*, Singapore, Singapore Academy of Law, p.180 *et seq.*

⁶⁴ Svantesson, J. & Zwieten, L., "Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution" *Computer Law & Security Review*, Volume 32 Issue 5, p.671 *et seq.*

⁶⁵ However, it is not always possible with absolute certainty to establish the geographical location of the server where the data is hosted. See in this regard: Svantesson, D., "Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution", retrieved from: https://cdn.ymaws.com/www.iisfa.net/resource/resmgr/Slide_seminari/Convegno_Milano/LEAccessSVANTESSON20160418SU.pdf p.8.

⁶⁶ See: Osula, A., Mutual Legal Assistance and Other Mechanisms for Accessing Extraterritorially Located Data, *Masaryk University Journal of Law and Technology*, Vol.9:1, 2015, p.44.

⁶⁷ See in more detail: Drake, W. J., Cerf, V. & Kleinwächter, W., *Internet Fragmentation: An Overview*, World Economic Forum Future of the Internet Initiative White Paper, Geneva, Switzerland: World Economic Forum, 2016, retrieved from: www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf, p.61.(04.07.2019).

for the Internet traffic on servers located in that particular country (case in point - Russia⁶⁸), or register under the national country code top-level domain.⁶⁹

That's why, in recent years a trend of voluntary cooperation between the public authorities from one state and private service providers in another state has occurred, mostly on the following actions: 1) domains seizures, 2) content takedown and 3) user data access.⁷⁰

2. LEGAL TIMELINE

In October 1995, the EU agreed on a Data Protection Directive (DPD) to harmonize differing national legislation on data privacy protection and establish a comprehensive EU-wide framework. The DPD provides that the transfer of personal data to a country outside of the EU may occur only if the European Commission determines that the country provides an adequate level of protection of personal data. The adequacy of the level of protection is assessed in the light of all the circumstances surrounding the data transfer; with particular consideration given to the nature of the data, the purpose and duration of the proposed processing operations, the countries of origin, and final destination of the data, and that country's laws, rules, and security measures.⁷¹ The DPD applies to all organizations, public and private, operating in the EU, including affiliates of US corporations. It covers the processing of all personal data, whether done automatically or manually.

But even today, EU does not have a single legal framework concerning the gathering, storage and transmission of electronic evidence. As a result, the police and the courts act in a uncertain environment, taking action that often contradicts the law, and the technological solutions *per se*. This could lead, for example: 1) to inadmissibility of the obtained evidence in the court proceedings; 2) the obsolescence of the technological devices/instruments/ software used by the law enforcement agencies since the criminal groups rapidly become aware of these tools and take swift countermeasures; 3) the non-existence of internationally binding rules and/or standards that should ensure admissibility of evidence gathered by one jurisdiction in the criminal proceedings in other jurisdiction etc.⁷² The cross – border crimes have specifics as to where the digital evidence be due to the information provider “recording” the information, where the actual digital information is stored and where the crime itself has a cross-border nature.⁷³ Among the first significant court cases where digital evidence was gathered and used in the proceedings were the *Yahoo!* case in Belgium and the *Rackspace* case in the UK, where the law-enforcement agencies directly requested e-evidence from a foreign-based provider.⁷⁴

⁶⁸ In 2014 the Russian Parliament enacted a Law obliging the Internet site to store Russian data on servers located in Russia or face blocking from the web by Roskomnadzor (Russian Internet watchdog agency). See: Anishchuk, A., “Russia passes law to force websites onto Russian servers”, retrieved from: <https://www.reuters.com/article/us-russia-internet-bill-restrictions/russia-passes-law-to-force-websites-onto-russian-serversidUSKBN0F91SG20140704>, (03.07.2019)

⁶⁹ See in this regard: Fehlinger, P., *Cyberspace Fragmentation: An Internet Governance Debate beyond Infrastructure.*, 2014, retrieved from: <https://policyreview.info/articles/news/cyberspace-fragmentation-internet-governance-debate-beyond-infrastructure/266>, (03.07.2019).

⁷⁰ De La Chapelle, B. & Fehlinger, P., “Jurisdiction on the Internet: from legal arms race to international cooperation,” *Global Commission on the Internet Governance Paper Series* No.28, 2016, p.6.

⁷¹ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data (Data Protection Directive).

⁷² Biasiotti, M., “Present and Future of Exchange of Electronic Evidence in Europe,” in: Biasiotti, M. A., Mifsud Bonnici, J. P., Cannataci, J., Turchi, F. (Eds), *Handling and Exchanging Electronic Evidence Across Europe*, Wien, Springer, 2018, p.13. *et seq.*

⁷³ Mifsud Bonnici J.P., Tudorica M., Cannataci J.A. (2018) The European Legal Framework on Electronic Evidence: Complex and in Need of Reform. In: Biasiotti M., Mifsud Bonnici J., Cannataci J., Turchi F. (eds) *Handling and Exchanging Electronic Evidence Across Europe*. Law, Governance and Technology Series, vol 39. Springer, Cham.

⁷⁴ Koops, B.&Goodwin, M., “Cyberspace, the cloud, and cross-border criminal investigation: The limits and possibilities of international law,” Tilburg Institute for Law, Technology, and Society, December 2014, retrieved from: https://www.wodc.nl/binaries/2326-volledige-tekst_tcm28-73009.pdf (accessed: 04.07.2019).

3.THE DRAFT REGULATION

On April 17, 2018 the Commission proposed a Regulation on the European Production (EPdO) and Preservation Orders (EpsO) for electronic evidence in criminal matters.⁷⁵ Both Orders need to be issued or validated by a judicial authority of a Member State. They can be served on providers of electronic communication services, social networks, online marketplaces, other hosting service providers and providers of internet infrastructure such as IP address and domain name registries, or on their legal representatives where they exist.⁷⁶ The latter represents a “new dimension in mutual recognition, beyond the traditional judicial cooperation in the Union, so far based on procedures involving two judicial authorities, one in the issuing State and another in the executing State.”⁷⁷ This is most intrusive procedural instrument available under the Regulation since it enables direct access to a service provider by the public authorities without the help of an intermediary.

The European Preservation Order is particularly designed to preserve the data in view of a subsequent request to produce this data existing at the time when the request was made (and not future data).⁷⁸ The remit concerns only data stored at servers at the moment of the receipt of the order. Real-time interception of telecommunication is thus excluded from these orders and that data should be requested via the European Investigation Order or the EU Mutual legal assistance agreement.⁷⁹

This newly proposed Regulation is enabling a competent authority of a Member State to order a service provider offering services in the Union, to produce or preserve electronic evidence, regardless of the location of the data. When issuing European Production and Preservation Orders, a respect must be ensured for the fundamental rights and legal principles as enshrined in Article 6 of the TEU, including the rights of defence of persons subject to criminal proceedings, and any obligations incumbent on law enforcement or judicial authorities in this respect shall remain unaffected.⁸⁰ The Regulation recognizes that requirement for double criminality is increasingly considered as an obstacle to smooth judicial cooperation, so EPOC may be issued for all criminal offences regardless of whether there are similar criminal offences established in other Member States or not.⁸¹

An important characteristic of the proposed Regulation is its significant effect on third countries.

Who can issue an European Production and European Preservation Order? According to the proposed Regulation, the competent authority can be: a) a judge, a court, an investigating judge or prosecutor competent in the case concerned or b) it can be issued by other authority determined by the issuing State which, is acting as an investigating authority in criminal proceedings with a view of gathering evidence for a specific case. This will include all authorities which have competence under national law to gather digital evidence. In such case, the order should be validated, by a judge, a court, an investigating judge or a prosecutor in the issuing State.⁸² As a result, it can happen for example 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.⁸³

A general pre-requisite for issuing both the EPdOs and EPsOs is that there should be criminal proceedings initiated regardless whether it is in trial or pre-trial phase, including when such proceedings are directed against legal persons. It does not matter whether such legal person can be held liable under national law - the order still must be executed. Also, for issuing both the EPdOs and EPsOs another general condition is that such issuance must be “necessary and proportionate” for the ongoing criminal proceedings in the requesting state. But for the EPdOs, special condition is that such order can be granted only if can be granted under a similar domestic situation in the issuing state for the same criminal offence. However, this provision could potentially trigger legislative changes in those Member States where such possibility does not exist in the moment i.e. by extending the possibilities to ask for production of subscriber or access data under national law.

⁷⁵ COM/2018/225 final - 2018/0108 (COD).

⁷⁶ European Commission, Explanatory Memorandum, Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final, 17.4.2018.

⁷⁷ European Data Protection Board, Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters (Art. 70.1.b), 26 September 2018, p.4.

⁷⁸ Ibid.

⁷⁹ De Busser, E., “EU-US Digital Data Exchange to Combat Financial Crime: Fast is the New Slow”, *German Law Journal*, Vol.19 No.05, p.1261.

⁸⁰ Art.1.

⁸¹ Art. 5 (3) and Art. 6 (2) of the Draft Regulation.

⁸² Art.4.

⁸³ Tosza, S., “The European Commission’s Proposal on Cross-Border Access to E-Evidence Overview and Critical Remarks,” *EUCrim* 4/2018.

But, on the other hand, while the requests to produce subscriber data or access data are available without limitations for all criminal offences, the Orders for releasing of transactional data or content data can be issued only if following strict conditions are met:

(1) for criminal offences punishable in the issuing State by a custodial sentence of a maximum of at least 3 years, or alternatively

(2) for the following offences, if they are wholly or partly committed by means of an information system:

–offences as defined in Articles 3 (offences related to computers), 4 (specifically adapted devices) and 5 (participation, instigation and attempt) of the Council Framework Decision 2001/413/JHA;

–offences as defined in Articles 3 to 7 of Directive 2011/93/EU (offences concerning sexual abuse and exploitation, child pornography, solicitation of children, and incitement, aiding and abetting and attempt);

–offences as defined in Articles 3 to 8 of Directive 2013/40/EU;

(c) for criminal offences as defined in Article 3 to 12 and 14 of Directive (EU) 2017/541 (offences regarding terrorist offences and participation in a terrorist group).⁸⁴

As a measure of caution, in cases where the data sought is stored or processed as part of an infrastructure provided by a service provider to a company or another entity other than natural persons, the European Production Order may only be addressed to the service provider where investigative measures addressed to the company or the entity are not appropriate, in particular because they might jeopardise the investigation.

By way of exception, in a case where an authority of the issuing Member States has suspicion whether transactional or content data requested are privileged or have immunities according to the national law of the Member State where the service provider is addressed, or may jeopardize the national security and defence, then it must request clarification by the competent authorities of the Member State concerned, communicating either directly or via Eurojust or the European Judicial Network. The European Production Order will not be issued if the named concerns are confirmed.⁸⁵

The conditions for issuing of an European Preservation Order are more liberal than those for the European Production Order: it can be issued whenever there is a need to prevent the removal, deletion or alteration of data in view of a subsequent request for production of this data via mutual legal assistance, a European Investigation Order or a European Production Order. These orders can be issued for all criminal offences.⁸⁶ It is important that the new Regulation makes gradation with regard of the sensitiveness of the data requested: subscriber and access data are less sensitive, while transactional and content data are more sensitive. As such, the latter are put onto a more protective legal regime. This regime applies only to preservation orders and these orders when seeking transactional content data must be rendered by a judge, a court, or an investigative judge and can be issued only for more serious criminal offences (carrying custodial sentence of a maximum of at least 3 years or fraudulent money transfers, offenses related to sexual abuse and exploitation of children and terrorism offenses wholly or partly committed by means of an information system).

It is also important to guarantee the immunity from liability, since the Recital 46 of the Regulation states that providers should be immune from liability for their good-faith compliance with disclosure and preservation orders, but such guarantee is not included in the operative part of the Regulation.

The proposed Regulation imposes strict time-limits for execution of the EPOCs and EPOC-PRs and also sanctions for the defaulting parties. So, the competent organ of the requested States is obliged to transmit the requested data at the latest within 10 days upon receipt of the EPOC, unless the issuing authority requested earlier disclosure. In emergency cases, the time-limit is maximum 6 hours from the receipt of the EPO. In comparison, under Directive on EIO the time-limit is 120 days or 10 months for a Mutual Legal Assistance procedure.

However, there are exceptions from these deadlines: firstly, if the EPOC is incomplete, contains manifest errors or does not contain sufficient information for its execution, then the addressee must inform the issuing authority without delay, and the latter must respond within 5 days at the latest; secondly, if *force majeure* appeared or of *de facto* impossibility occurred (the person whose data is sought is not their customer or the data has been deleted before receiving the EPOC), the addressee will inform the issuing authority without delay and the latter in this case is expected to withdraw the EPO.

If the EPOC cannot be executed because (in the opinion of the addressee) it manifestly violates the Charter of Fundamental Rights or if it is manifestly abusive, the addressee shall inform the competent enforcement authority of

⁸⁴ Art.5.

⁸⁵ Art.5(7).

⁸⁶ Art.6.

its Member State. Then, the latter may seek clarifications from the issuing authority on the European Production Order, directly or through Eurojust or the European Judicial Network.⁸⁷

On the other hand, when a EPOC – PR is received by the addressee, it must immediately preserve the data requested, and is obliged to keep the data for a maximum period of 60 days, unless the issuing authority confirms that EPO will be served. Also, if the need for the requested data ceases to exist, the issuing authority must inform the addressee without delay. The rules in an event of non-execution of the Order are the same as the rules in the similar cases of EPO. Also, in any other cases where the addressee did not preserved the requested data, he will inform the issuing authority without delay.⁸⁸

For unjustified non-execution of both the European Production and Preservation Orders, the Member States should impose pecuniary sanctions which should be “effective, proportionate and dissuasive.”⁸⁹

In an event of non-compliance within the set time-limits by the Regulation, or the addressee does not provide justified reasons for the non-execution, the European Production Order and the European Preservation Order can be forwarded to the enforcing authority in the Member State concerned, which should immediately validate the Order, and no later than 5 days. The enforcing authority can oppose the execution only if data concerned is protected by an immunity or privilege under its national law or its disclosure may impact its fundamental interests such as national security and defence.⁹⁰ The addressee is then required within new time-limit set by the enforcing authority to execute the Order, and must be informed that non-compliance entails financial penalties and also for the possibility not to comply from the following reasons: A) common for the Production and the Preservation Order: 1) they have not been issued or validated by an issuing authority as provided for in Article 4; 2) *de facto* impossibility or *force majeure*, or because the Orders contain manifest errors; 3) they do not concern data stored by or on behalf of the service provider at the time of receipt of Orders; 4) the services do not fall within the purview of the present Regulation; 5) it is apparent that the Orders manifestly violate the Charter or is manifestly abusive; B) Unique for the European Production Order: 1) it has not been issued for an offence provided for by Article 5(4).⁹¹

Both the European Production and Preservation Orders can potentially affect the fundamental human rights like: 1) of the suspected or indicted person: right to protection of personal data; right to respect of private and family life; right to freedom of expression; right of defence; right to an effective remedy and to a fair trial; 2) of the service provider: right to freedom to conduct a business; right to an effective remedy; 3) rights of all citizens: right to liberty and security. During the pre-trial and trial phase, all criminal law procedural safeguards available under EU law are applicable: the right to a fair trial enshrined in Article 6 ECHR and Articles 47 and 48 of the Charter of Fundamental Rights; the rights enjoyed under Directive 2010/64/EU on the right to interpretation and translation in criminal proceedings, Directive 2012/13/EU on the right to information about rights and charges and access to the case file, Directive 2013/48/EU on the right of access to a lawyer and communication with relatives when arrested and detained, Directive 2016/343 on the strengthening of certain aspects of the presumption of innocence and the right to be present at one’s trial, Directive 2016/800 on the procedural safeguards for children and Directive 2016/1919 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings.

4. LEGAL REMEDIES

Besides the aforementioned rights, the proposed Regulation sets three specific types of legal remedies against issued Production and Preservation Orders: 1) *Review procedure in case of conflicting obligations based on fundamental rights or fundamental interests of a third country*, 2) *Review procedure in case of conflicting obligations based on other grounds* and 3) *Effective remedies (available for the accused or suspected persons)*. Only the remedies for the service providers are enshrined in the draft – Regulation. The remedies for all other affected persons should be provided by national law and should include the possibility to challenge legality of the measure (including proportionality and necessity, infringement of the rights enshrined in the EU Charter) before the national courts.

The real innovation in the proposed Regulation—and a similarity with the US CLOUD Act—is the recognition of potential conflicts of laws affecting the companies involved. Such situations created legal uncertainty for the

⁸⁷ Art.9.

⁸⁸ See: De Busser, E., *op.cit.*, p.1262.

⁸⁹ Art.13.

⁹⁰ Art.9(2).

⁹¹ Art.14 (4)&(5).

companies. Besides this, waste of time and resources occurred since the issuing authority had to resort to other ways to gather the requested evidence in a ongoing criminal investigation.⁹²

The first remedy governed by Art.15, can be initiated by lodging a reasoned objection by the addressee to the issuing authority when the Order conflicts the applicable laws 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 related to national security or defence. The issuing authority can accept the objection and revoke the order, but if it upholds the Order, then it must seek judicial review, during which the order will be suspended. The national court should focus whether the third country laws are applicable to the facts of the case and whether it prohibits the disclosure of the data concerned. Particularly, the court will assess whether the third country law is enacted to protect other interests or just shields the illegal activities from requests by law enforcement agencies. If the court established that such conflict exists it will communicate the case-file to the central authorities of the third country with a deadline of 15 days to object (extendable to 30). If the central authorities do object to the order, the court will lift the order and inform subsequently the issuing authority and the addressee. But if there is no objection the court will uphold order, and then the addressee must proceed with the execution.⁹³

Article 16 regulates the situation when conflicts with grounds other those enlisted in Art.15 exist. Then the procedure is the same, with exception with the judicial stage when the competent court must assess whether:

a) the interest protected by the relevant law of the third country, including the third country's interest in preventing disclosure of the data;

(b) the degree of connection of the criminal case for which the Order was issued to either of the two jurisdictions, as indicated *inter alia* by: the location, nationality and residence of the person whose data is being sought and/or of the victim(s), the place where the criminal offence in question was committed;

(c) the degree of connection between the service provider and the third country in question; in this context, the data storage location by itself does not suffice in establishing a substantial degree of connection;

(d) the interests of the investigating State in obtaining the evidence concerned, based on the seriousness of the offence and the importance of obtaining evidence in an expeditious manner;

(e) the possible consequences for the addressee or the service provider of complying with the European Production Order, including the sanctions that may be incurred.⁹⁴

If the competent court upholds the Order then the addressee must proceed with the execution. The persons against whom the criminal investigations or criminal proceedings are conducted have a right to challenge both the European Production Order and European Preservation Order. This is without prejudice to their rights available under Directive (EU) 2016/680 - like the rights to: 1) lodge a complaint with a supervisory authority, 2) an effective judicial remedy against a supervisory authority, 3) an effective judicial remedy against a controller or processor, 4) right to mandate a not-for-profit body, organisation or association to lodge the complaint on his or her behalf and to exercise these rights, and Regulation (EU) 2016/679 - like the rights to: 1) to lodge a complaint with a supervisory authority, 2) an effective judicial remedy against a supervisory authority, 3) an effective judicial remedy against a controller or processor, 4) Representation of data subjects etc.

Also, the same rights will be enjoyed by other persons whose data has been obtained, but they were not suspects or indicted persons in the proceedings. The challenge of the European Production Order should be exercised before the competent courts of the issuing state within the time-limits set by the national law in comparable situations. There is an additional obligation for the Member States to ensure that "rights of the defence and the fairness of the proceedings are respected when assessing evidence obtained through the European Production Order".⁹⁵

The competent court in the Member State of the addressee must assess whether the transactional or content data obtained by the European Production Order is protected by immunities or privileges, as well as whether it affects the national security and defence, in the same way when it assesses similar measures in comparable domestic situations. The court may consult the authorities of the relevant Member State, the European Judicial Network in criminal matters or Eurojust.

⁹² De Busser, *op.cit.*, p.1262.

⁹³ Art.15.

⁹⁴ Art.16.

⁹⁵ Art.17.

5.CONCLUSION

The newly proposed Regulation on European Production and Preservation Orders will inevitably represent a major advancement in the application of the principle of mutual recognition. It is increasingly important that the proposed regime largely corresponds to the newly established regime under the US CLOUD Act, since the gross proportion of all requests for e-evidence are directed towards US service providers. However, the proposed text raises concern on some issues. For instance, the LIBE Committee of the EP made sustained remarks regarding: 1) the hybrid sanctions regime, which mostly resembles a Directive, rather than a Regulation; the danger of forum-shopping by appointing legal representatives by the service providers in those Member States with minimal sanctions and the need of establishing at least a minimum penalties by the Regulation in order to avoid that; 2) the unrealistic time limits for transmitting the required data by the providers: either two separate deadline-regimes to be introduced, one for the big companies and one for SMEs or, if decided to stick to a single regime for all, deadlines need to be longer than those set by the Commission in its proposal; 3) the danger that the service providers will interpret the grounds for refusal too broadly in order to appeal to clients and engage in litigation before the courts (particularly the more economically viable providers). There are no specific rules to ensure integrity of the requested electronic data before and during the process of collection. Also, there is no restriction of the access and subscriber data for specifically listed criminal offences, nor there is a sufficient threshold for issuing and executing requests for content data, particularly due to the fact that there will be no control by a judicial authority in the Member State where the data is stored. There is no safety mechanism that will ensure actual reimbursement of costs for the service providers from the issuing Member States. With exception to some basic metadata, the further involvement of prosecutors in issuance or authorization of such requests is questionable, since both the CJEU⁹⁶ and ECtHR⁹⁷ has held that they do not consider that prosecutors are fulfilling the criteria of independence. It remains to be seen whether these issues will be addressed in the legislative process.

REFERENCES

- Anishchuk, A., "Russia passes law to force websites onto Russian servers", retrieved from: <https://www.reuters.com/article/us-russia-internet-bill-restrictions/russia-passes-law-to-force-websites-onto-russian-serversidUSKBN0F91SG 20140704>. (03.07.2019).
- Biasiotti, M., "Present and Future of Exchange of Electronic Evidence in Europe," in: Biasiotti, M. A., Mifsud Bonnici, J. P., Cannataci, J., Turchi, F. (Eds), *Handling and Exchanging Electronic Evidence Across Europe*, Wien, Springer, 2018.
- De Busser, E., "EU-US Digital Data Exchange to Combat Financial Crime: Fast is the New Slow", *German Law Journal*, Vol.19 No.05.
- De La Chapelle, B. & Fehlinger, P., "Jurisdiction on the Internet: from legal arms race to international cooperation," *Global Commission on the Internet Governance Paper Series* No.28, 2016.
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data (Data Protection Directive).
- Drake, W. J., Cerf, V. & Kleinwächter, W., *Internet Fragmentation: An Overview*, World Economic Forum Future of the Internet Initiative White Paper, Geneva, Switzerland: World Economic Forum, 2016, retrieved from: ww3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf, p.61.(04.07.2019).
- European Data Protection Board, Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters (Art. 70.1.b), 26 September 2018.
- Fehlinger, P., *Cyberspace Fragmentation: An Internet Governance Debate beyond Infrastructure*, 2014, retrieved from: <https://policyreview.info/articles/news/cyberspace-fragmentation-internet-governance-debate-beyond-infrastructure/266>.(03.07.2019)
- Koops, B.&Goodwin, M., "Cyberspace, the cloud, and cross-border criminal investigation The limits and possibilities of international law," Tilburg Institute for Law, Technology, and Society, December 2014, retrieved from: https://www.wodc.nl/binaries/2326-volledige-tekst_tcm28-73009.pdf (accessed: 04.07.2019).
- Mason, S., "Some International Developments in Electronic Evidence", in: Kin, L. (ed.) *International Conference on Electronic Litigation*, Singapore, Singapore Academy of Law.

⁹⁶ Case C-203/14, *Consorti Sanitari del Maresme*, 6.10.2015.

⁹⁷ Application no. 37104/06, *Moulin v France*, 23.11.2010, ECHR, <http://hudoc.echr.coe.int/eng-press?i=003-3344651-3742609>.

- Mifsud Bonnici J.P., Tudorica M., Cannataci J.A. (2018), “The European Legal Framework on Electronic Evidence: Complex and in Need of Reform.” In: Biasiotti M., Mifsud Bonnici J., Cannataci J., Turchi F. (eds) *Handling and Exchanging Electronic Evidence Across Europe*. Law, Governance and Technology Series, vol 39. Springer, Cham.
- Osula, A., Mutual Legal Assistance and Other Mechanisms for Accessing Extraterritorially Located Data, *Masaryk University Journal of Law and Technology*, Vol.9:1, 2015.
- Svantesson, J. & Zwieten, L., “Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution” [Computer Law & Security Review](#), Volume 32 Issue 5.
- Svantesson, D., “Law enforcement access to evidence via direct contact with cloud providers – identifying the contours of a solution”, retrieved from: https://cdn.ymaws.com/www.iisfa.net/resource/resmgr/Slide_seminari/Convegno_Milano/LEAccess_SVANTESSON20160418SU.pdf p.8.
- Tosza, S., “The European Commission’s Proposal on Cross-Border Access to E-Evidence Overview and Critical Remarks,” *EUCrim* 4/2018.