Towards New European Regulation for Handling Electronic Evidence

Dobrinka Chankova, Ralitsa Voynova
South-West University, Blagoevgrad, Bulgaria

Gathering and using e-evidence in trans-border criminal investigation still faces many challenges which reflects the efficiency of crime counteraction. It has been long time a common concern of the legal community. The European Union has shown deep interest to the issue and has undertaken crucial measures. Recently, a proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders, for electronic evidence in criminal matters, and 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 have been launched after long and thorough preparation. Through these specific tools, the proposal targets the problem created by the volatile nature of electronic evidence and its international dimension. It seeks to adapt cooperation mechanisms to the digital age, giving the judiciary and law enforcement tools to address the way criminals communicate today and to counter modern forms of criminality. The proposal also aims to improve legal certainty for authorities, service providers, and persons affected and to maintain a high standard for law enforcement requests, thus ensuring protection of fundamental rights, transparency, and accountability. It also speeds up the process to secure and obtain electronic evidence that is stored and/or held by service providers established in another jurisdiction. This study outlines the basic achievements of the newly proposed regulation.

Keywords: e-evidence, European Production Order, European Preservation Order, criminal investigation, cooperation mechanisms, safeguards

Introduction

The massive use of Internet, social networks, and digital media has encouraged criminal practices. Today, cyber-crime covers a wide range of offences including bank and credit card fraud, hacking, sexual harassment, sextortion, bullying, copyright infringement, child pornography, and even so-called romance scams where people are persuaded to part with thousands of Euro/pounds/dollars by people posing as their lovers online. Moreover, cyber-attacks by sophisticated actors designed to disrupt essential services, like energy, water, and transport networks are a problem for national security. Cyber-crime has become a leading concern in the legal community as criminals continue to spread troublesome viruses, access private business/financial information, commit cyber-espionage and cyber-terrorism, spread different variation of malware, execute property and identity theft, and invade computer system processes that may threaten or cause danger to the government or its citizens.

Dobrinka Chankova, Ph.D., professor, Department of Public Law Sciences, Faculty of Law and History, South-West University, Blagoevgrad, Bulgaria.
Ralitsa Voynova, Ph.D., assistant professor, Department of Public Law Sciences, Faculty of Law and History, South-West University, Blagoevgrad, Bulgaria.
The legal community in European scale and globally has devised laws punishing cyber-crime. However, such provisions are never sufficient if the crime is not proved. With many cyber-criminals based overseas, it makes extremely difficult for the police to investigate and bring the perpetrators to justice. In many cyber-crime prosecutions, social media, webmail, messaging services, and applications are often the only place where investigators can find leads to determine who committed a crime and obtain evidence that can be used in court. The increased uses of e-evidence inevitably challenge the very concept of evidencing at present day. Hence, the electronic evidence handing is of utmost importance in many cases.

E-evidence are still a controversial issue in Europe and worldwide, more between practitioners than between theoreticians (Casey, 2004; Carrier, 2006). It comes from the very basic characteristics of digital evidence—its volatility. A powered electronic device modifies its state every time a specific event happens. Lack of power or a system overwriting old data with new data requires preserving electronic evidence as soon as possible. Furthermore, it may be altered or destroyed through normal use. Devices constantly change the state of memory—allocating it for programs automatically, swapping it to disk, or writing chunks of it to a disk file on user request. That is why the authenticity, admissibility, and reliability of e-evidence in criminal proceedings are crucial point, indeed. Laws regarding admissibility of evidence differ between countries. In certain countries, there are defined rules as to admissibility of evidence in legal proceedings, while in other countries, admissibility is flexible. Some countries have adapted their legislation to accommodate electronic evidence; others rely on traditional laws and apply them to e-evidence. There are thus significant differences in national legislations and approaches, which makes the handling of electronic evidence difficult across jurisdictions and creates legal and practical uncertainty. Evidence rules vary considerably even amongst countries with similar legal traditions. In certain countries, traditional investigative powers might be general enough to apply to electronic evidence; while in other traditional procedural laws, it might not cover specific issues regarding e-evidence, making it necessary to have additional legislation.2

In response, a number of member states of the EU and third countries have resorted to expanding their national tools. The result leads to further fragmentation of legal frameworks which generated greater legal uncertainties and conflicting obligations and raised questions about the protection of fundamental rights and procedural safeguards for persons affected. Therefore, there was ascertained a need to put forward a European legal framework for electronic evidence to impose an obligation on service providers to respond directly to authorities without the involvement of a judicial authority in the member state of the service provider. For situations where either the evidence or the service provider is located elsewhere, mechanisms for cooperation between countries were developed several decades ago3. In the EU, mutual recognition mechanisms now are mainly based on the European Investigation Order Directive4; and with third countries, mutual legal assistance

1 Council of Europe’s Convention of Cyber-Crime, CETS No.185, Budapest, 23 November 2001, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185; Directive 2013/40/EU on attacks against information systems; OJ L 218, 14.8.2013; Title 18 of the U.S. Criminal code, https://www.law.cornell.edu/uscode/text/18/part-I, Last accessed 28 August 2018, Penal Code of the Republic of Bulgaria 1968, last amended State Gazette N. 55/2018, etc.
2 The admissibility of electronic evidence in court. Fighting against high-tech crime, Cybex Initiative. With financial support from the AGIS Programme of the European Commission, Barcelona, 2006.
3 For example, Europol, Eurojust, European Judicial Network, etc. have been created.
4 Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014.
mechanisms. However, the new situation poses new challenges. In 2016, the Council of the EU called for concrete action based on a common EU approach to make mutual legal assistance more efficient; to improve cooperation between member state authorities and service providers based in non-EU countries; and to propose solutions to the problem of determining and enforcing jurisdiction in cyberspace. The European Parliament similarly highlighted the challenges that the current legal framework can create for service providers seeking to comply with law enforcement requests and called for a European legal framework, including safeguards for the rights and freedoms of all concerned. The new rules are the outcome of a two-year process resulting from strong calls for action by EU member states and industry. It included a thorough impact assessment analysing the problem, supported by extensive stakeholder consultations, including a public consultation. To make it easier and faster for law enforcement and judicial authorities to obtain the electronic evidence they need to investigate and eventually prosecute criminals and terrorists, the European Commission proposed on 17 April 2018 new rules in the form of a “Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters” and 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.” As according to the standard European practice, the final approval of these documents is only a question of time. This study will explore some of the most important achievements of the regulation and the directive as they deserve a special attention.

Basic Provisions of the Regulation—Subject Matter, Definitions and Scope

According to Article 1 “This regulation lays down the rules under which an authority of a member state may order a service provider offering services in the Union, to produce or preserve electronic evidence, regardless of the location of data...”. The explanatory memorandum adds that it could be done through European Production or European Preservation Order. These instruments, which are the biggest novelty of the new proposal and are further explained in details, can only be used in cross-border situations, that is, in situations where the service provider is established or represented in another member state. In such way, the regulation shall give additional tools to investigating authorities to obtain electronic evidence without limiting the powers that already set out by national law to compel service providers established or represented on their territory. If the service provider is established or represented in the same member state, authorities of that member state shall therefore use national measures to compel the service provider. The data ordered through a European Production Order should be provided directly to the authorities without the involvement of authorities...

---

5 Council Act of 29 May 2000 establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, OJ C 197/01, 12.07.2000; Council Decision 2009/820/CFSP of 23 October 2009 on the conclusion on behalf of the European Union of the Agreement on extradition between the European Union and the United States of America and the Agreement on mutual legal assistance between the European Union and the United States of America, OJ L291/40, 7.11.2009; Council Decision 2010/616/EU of 7 October 2010 on the conclusion of the Agreement between the European Union and Japan on mutual legal assistance in criminal matters, OJ L 271, 15.10.2010, etc.

6 Conclusions of the Council of the European Union on improving criminal justice in cyberspace, ST9579/16, https://www.consilium.europa.eu/media/24300/cyberspace-en.pdf, Last accessed 4 September 2018.

7 P8_TA (2017) 0366, http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P8-TA-2017-0366, Last accessed 4 September 2018.

8 COM/2018/225 final-2018/0108 (COD), https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2018%3A225%3AFIN, Last accessed 4 September 2018.

9 COM/2018/226 final-2018/0107 (COD), https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2018%3A226%3AFIN, Last accessed 4 September 2018.
in the member state where the service provider is established or represented. The regulation also moves away from data location as a determining connecting factor, as data storage normally does not result in any control by the state on whose territory data is stored. Such storage is determined in most cases by the provider alone, on the basis of business considerations. Moreover, the regulation is also applicable if the service providers are not established or represented in the EU, but offer services in the Union (Article 3(1)).

Article 2 sets out definitions which apply throughout the instrument. The most important and used are the following:

“European Production Order” means 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.

“European Preservation Order” means 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.

“Service provider” means any natural or legal person who provides one or more of the explicitly mentioned categories of services: electronic communications services, information society services for which the storage of data is a defining component of the service provided to the user, including social networks to the extent they do not qualify as electronic communications services, online marketplaces facilitating transactions between their users (such as consumers or businesses) and other hosting service providers, and providers of internet domain name and numbering services.

Sometimes, the regulation refers to a specific meaning of “establishment”, that is why it gives explanation of it: “Establishment” means either the actual pursuit of an economic activity for an indefinite period through a stable infrastructure from where the business of providing services is carried out or a stable infrastructure from where the business is managed.

These definitions are of ultimate importance for clear understanding and right application of the instrument. But the real value is the definition of e-evidence. In the theory and in some soft-law documents, there is long lasting debate what exactly the e-evidence is. Each of proposed definitions highlights some, but not all, essential features, and sometimes, this is confusing.

Usually as e-evidence are considered any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offenses, such as intent or alibi (Carrier, 2006).

According to a large European Evidence Project, electronic evidence is any data resulting from the output of an analogue device and/or a digital device of potential probative value that are generated by, processed by, stored on, or transmitted by any electronic device (Biasiotti, Epifani, & Turchi, 2015).

Not on a final place, as e-evidence is considered the information stored or transmitted in a binary form that may be relied on in court (Ashcroft, Daniels, & Hart, 2004).

The definition of the regulation is significantly improved and more practical: “Electronic evidence” means evidence stored in electronic form by or on behalf of a service provider at the time of receipt of a production or preservation order certificate, consisting in stored subscriber data, access data, transactional data, and content data. All these data are further explained but could be resumed that the first three categories are commonly referred as “non-content data” and the last one have in mind stored content data. All categories contain personal data and are thus covered by the safeguards under the EU data protection acquis. The intensity of the impact on
fundamental rights varies between them, in particular between subscriber data, and on the one hand, transactional and content data on the other hand. It is essential that all these categories are covered by the instrument: Subscriber and access data are often the starting point to obtain leads in an investigation about the identity of a suspect, while transactional and content data can be the most relevant as probative material. Because of the different levels of interference with fundamental rights, it is justified to attach different conditions to subscriber data on the one hand and transactional and content data on the other hand, as is done in several provisions in the regulation.

The scope of regulation is stipulated in Article 3—the instrument applies to service providers which offer services in the Union. The European Production Orders and European Preservation Orders may only be issued for criminal proceedings, both during the pre-trial and trial phase. The orders may also be issued in proceedings relating to a criminal offence for which a legal person may be held liable or punished in the issuing state. That means that the regulation does not cover crime prevention or other proceedings or disorders, such as administrative proceedings for infringements of the law. Furthermore, it does not require service providers to systematically collect or store more data than are necessary for commercial reasons or in accordance with other legal requirements.

**European Production Order, European Preservation Order and Certificates**

When issuing a European Production or Preservation Order, a judicial authority always needs to be involved as either an issuing or a validating authority. The proposed regulation distinguishes production orders to produce transactional and content data, from those concerning subscriber or access data. More precisely, according to Article 4, a European Production Order for subscriber data and access data may be issued by a judge, a court, an investigating judge, or prosecutor competent in the case concerned; or 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 European Production Order shall be validated, after examination of its conformity with the conditions for issuing a European Production Order under the Regulation, by a judge, a court, an investigating judge, or a prosecutor in the issuing state. A European Production Order for transactional and content data may be issued only by: a judge, a court, or an investigating judge competent in the case concerned (without prosecutor); or any other competent authority, accordingly. For the European Preservation Order, the rules for the production order apply.

Article 5 sets out the conditions for issuing a European Production Order. They have to be assessed by the issuing judicial authority. The European Production Order may only be issued if this is necessary and proportionate in the individual case. Moreover, it should only be issued if a similar measure would be available in a comparable domestic situation in the issuing State. Orders to produce subscriber data and access data can be issued for any criminal offence. Transactional and content data should be subject to stricter requirements to reflect the more sensitive nature of such data and the correspondingly higher degree of invasiveness of orders for such data, as compared to subscriber and access data. Orders can therefore only be issued for offences which carry a maximum custodial sentence of at least three years or more. Setting a threshold based on the maximum custodial sentence allows for a more proportionate approach, together with a number of other *ex ante* and *ex post* conditions and safeguards to ensure respect for proportionality and the rights of the persons affected. In addition, orders to provide transaction data or content data may also be issued for some specific harmonized
offenses listed in Article 5 of the regulation, for which evidence is normally only available in electronic form. This justifies the application of the regulation and in cases where the maximum period of imprisonment is shorter than three years.

A European Preservation Order is subject to similar conditions as the European Production Order. It is explicitly stated in Article 6(2) that it may be issued where necessary and proportionate 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. European Preservation Orders to preserve data may be issued for all criminal offences.

European Production Orders and European Preservation Orders should be addressed to a legal representative designated by the service provider for the purpose of gathering evidence in criminal proceedings in accordance with the proposed directive, laying down harmonised rules on the appointment of these representatives (Article 7). The transmission will be in form of a European Production Order Certificate (EPOC) or a European Preservation Order Certificate (EPOC-PR) as referred to in Article 8. This legal representative will be responsible for their reception and timely and complete execution. This leaves service providers the choice of how to organise themselves to produce the data ordered by member state authorities. Where no legal representative has been appointed, orders may be addressed to any establishment of the service provider in the EU.

The issuing or validating authority shall complete the EPOC set out in Annex I or the EPOC-PR set out in Annex II, shall sign it and shall certify its content as being accurate and correct. The EPOC or the EPOC-PR shall be directly transmitted by any means capable of producing a written record under conditions allowing the addressee to establish its authenticity. Where service providers, member states or Union bodies have established dedicated platforms or other secure channels for the handling of requests for data by law enforcement and judicial authorities, the issuing authority may also choose to transmit the certificate via these channels.

The time limits for the execution of an EPOC is the next important benefit of this tool. Article 9 of the regulation says that upon receipt of the EPOC, the addressee shall ensure that the requested data is transmitted directly to the issuing authority or the law enforcement authorities as indicated in the EPOC at the latest within 10 days, unless the issuing authority indicates reasons for earlier disclosure. In emergency cases, the addressee shall transmit the requested data without undue delay, at the latest within six hours upon receipt of the EPOC. For comparison, this time limits are up to 120 days for the existing European Investigation Order or an average of 10 months for a mutual legal assistance procedure. Upon receipt of the EPOC-PR, the addressee shall, without undue delay, preserve the data requested. The preservation shall cease after 60 days, unless the issuing authority confirms that the subsequent request for production has been launched.

The regulation also provides for an official dialogue between the addressee and the issuing authority, which is another guarantee for the effectiveness of the new instrument for obtaining evidence. More specifically, if the EPOC is incomplete, clearly inaccurate, or does not contain sufficient information to enable the service provider to complete it, the addressee shall contact the issuing authority and request clarification.

---

10 These offences are listed in the specific provisions of: Council Framework Decision 2001/413/JHA combating fraud and counterfeiting of non-cash means of payment; Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography; Directive 2013/40/EU on attacks against information systems; Directive 2017/541/EU on combating terrorism.
using the form set out in Annex III. Respectively, if the addressee does not provide the information at all or does not provide comprehensive information or does not provide it within the required time limit due to force majeure or de facto impossibility, it must notify the issuing authority of the reasons using the same form.

Safeguards

The new rules guarantee, simultaneously with the improvement of the procedures concerning e-evidence, strong protection of fundamental rights including safeguards for the right to protection of personal data. The service providers and persons whose data are being sought will benefit from various safeguards and be entitled to legal remedies. Addressees and, if different, service providers shall take the necessary measures to ensure the confidentiality of the EPOC or the EPOC-PR and of the data produced or preserved and where requested by the issuing authority, shall refrain from informing the person whose data is being sought in order not to obstruct the relevant criminal proceedings (Article 11).

The confidentiality of the ongoing investigation, including the fact that there has been an order to obtain relevant data, is also protected. This is inspired by Article 19 of the European Investigation Order (EIO) Directive and Article 23 of General Data Protection Regulation. From the whole regulation is evident the sensitivity of the EU legislation which strictly protects the rights of the suspects and the accused in criminal proceedings, and there are already many rules to protect personal data. However, for the persons whose data is being sought, these additional safeguards in the proposal provide extra procedural rights. These include the possibility to challenge the legality, necessity, or the proportionality of the order without restricting the grounds for the challenge in accordance with national law. The rights under the law of the enforcing state are fully respected by ensuring that immunities and privileges which protect the data sought in the member state of the service provider are taken into account in the issuing state. This is especially the case where they provide for a higher protection than the law of the issuing state. On the other hand, it is important, including for exercising legal remedies, that the person whose data was sought, is informed. Where this is not done by the service provider upon request of the issuing authority, the issuing authority shall inform the person in accordance with Article 13 of the Law Enforcement Data Protection Directive once there is no longer a risk of jeopardising the investigation and include information about available legal remedies. Because of the lesser interference with rights involved, such information is not provided for in case of a European Preservation Order, but only for European Production Orders. As mentioned, personal data covered by this proposal are strictly protected and may only be processed in accordance with the General Data Protection Regulation and the Data Protection Directive for Police and Criminal Justice Authorities (Law Enforcement Data Protection Directive). Unlike surveillance measures or data retention obligations set out by law, which are not provided for by this Regulation, the European Preservation Order is an Order issued or validated by a judicial authority in a concrete criminal procedure after an individual evaluation of the proportionality and necessity in every single case. Like the European Production Order, it refers to the specific known or unknown perpetrators of a criminal

11 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016.
12 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016.
offence that has already taken place. The European Preservation Order only allows preserving data that are already stored at the time of receipt of the Order, not the access to data at a future point in time after the receipt of the European Preservation Order.

Both orders can be used only in criminal proceedings, from the initial pre-trial investigative phase until the closure of the proceedings by judgment or other decision. In addition, a specific procedure is set up for situations where the obligation to provide data conflicts with a competing obligation arising from a third country law on other grounds (Chapter 4).

Member states’ authorities may continue to issue European Investigation Orders in accordance with Directive 2014/41/EU for the gathering of evidence that would also fall within the scope of the regulation. The new instrument will not replace the EIO for obtaining electronic evidence but provides an additional tool for authorities. There may be situations, for example when several investigative measures need to be carried out in the executing member state, where the EIO may be the preferred choice for public authorities. Creating a new instrument for electronic evidence is a better alternative than amending the EIO Directive because of the specific challenges inherent in obtaining electronic evidence which do not affect the other investigative measures covered by the EIO Directive. This regulation should be applied without prejudice to the procedural rights in criminal proceedings set out in other directives of the European Parliament and of the Council.¹³

The final provisions reasonably provides monitoring and reporting and evaluation. The rules in the Regulation are envisaged to be supplemented by the provisions of the proposed directive which oblige service providers to designate a legal representative in the Union: To ensure that all providers that offer services in the Union are subject to the same obligations, even if their headquarters are in a third country, they are required to designate a legal representative in the Union for the receipt of, compliance with and enforcement of decisions and orders. In such way, it could be provided legal certainty for businesses and service providers, whereas today law enforcement authorities often depend on the good will.

Conclusion

The mechanism of the European Production Order and the European Preservation Order for electronic evidence in criminal matters can only work on the basis of a high level of mutual trust between the member states, which is an essential precondition for the proper functioning of the proposed regulation. An authority in the country where the addressee of the order is located will not have to be involved in serving and executing the order directly, except if there is non-compliance, in which case enforcement will be required and the competent authority in the country where the representative is located will intervene. The building of enhanced cooperation between member states in the field of criminal law and criminal investigation is ongoing but deepening process and a warranty for the successful application of this instrument. In such a way, better and faster handling of e-evidence will be achieved, the efficiency of crime counteraction will be raised, and victim protection will be improved.

The regulation strongly respects also the fundamental rights and observes the principles recognised in particular by the Charter of Fundamental Rights of the European Union. These include the right to liberty and

¹³ Directive 2012/13/EU on the right to information in criminal proceedings, OJ L 142, 1.6.2012; Directive 2013/48/EU on the right of access to a lawyer and communication with relatives when arrested and detained OJ L 294, 6.11.2013; Directive 2016/1919 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings, OJ L 297, 4.11.2016, etc.
security, the respect for private and family life, the protection of personal data, the freedom to conduct a business, the right to property, the right to an effective remedy and to a fair trial, the presumption of innocence and right of defence, the principles of the legality and proportionality. In order to guarantee full respect of fundamental rights, this regulation explicitly refers to the necessary standards regarding the obtaining of any personal data, the processing of such data, the judicial review of the use of the investigative measure provided by this instrument and the available remedies. The only thing that left is its full implementation by member states and, why not, beyond.

References
Ashcroft, J., Daniels, D. J., & Hart, S. V. (2004). *Forensic examination of digital evidence: A guide for law enforcement* (1st ed.). Washington, DC: National Institute of Justice U.S. Department of Justice, Office of Justice Programs, National Institute of Justice.

Biasiotti, M., Epifani, M., & Turchi, F. (2015). The evidence project: Bridging the gap in the exchange of digital evidence across Europe, In *Proceedings of the 10th International Conference on Systematic Approaches to Digital Forensic Engineering* (SADFE 2015), September 30-October 2, Malaga, Spain.

Carrier, B. D. (2006). A hypothesis-based approach to digital forensic investigations (Ph.D. thesis, Purdue University). Retrieved from [https://www.cerias.purdue.edu/tools_and_resources/bibtex_archive/archive/2006-06.pdf](https://www.cerias.purdue.edu/tools_and_resources/bibtex_archive/archive/2006-06.pdf)

Casey, E. (2004). *Digital evidence and computer crime* (2nd ed.). Amsterdam: Elsevier Academic Press.