A New Legal Framework for Cross-Border Data Collection in Crime Investigation amongst Selected European Countries

Borka Jerman-Blažič & Tomaž Klobučar
Jožef Stefan Institute, Slovenia

Abstract
This paper presents the current issues and proposes legal remedies for removing the barriers to gathering cross-border electronic evidence for a more efficient fight against crime and cybercrime. It presents the legal scene in the EU, the efforts related to the implementation of the Directive 2014/41/EU regarding the European Investigation Order in criminal matters, and the provision of legal procedures for e-evidence collection proposed within the EU proposal for the Directive for orders to preserve and produce evidence related to criminal acts in a territory different from the location of the crime act. The results of the EU LIVE_FOR project intended to raise the awareness and improve the implementation of the Directive 2014/41/EU are presented as well. Finally, the procedures proposed in the new EU regulation for collecting e-evidence are analysed and the expected removal of juridictive barriers for a more efficient justice processing of crime acts in an interconnected world assessed.

Keywords: E-evidence, crime, investigation order, production order, preservation order.

Introduction
The interconnectivity of the global economy enables criminals to operate trans-jurisdictionally, with the elements connected to their crimes spread widely across the globe in both time and space (Herrera-Flanigan & Ghosh, 2010). More and more crimes are committed online today, facilitated by computing devices such as mobile phones, tablets, or PCs. The nature of these devices allows that traces associated with crime are left. That is why electronic forms of evidence for judicial proceedings are increasingly in demand today. Digital devices store, transmit, or process a wealth of user data that is integrated with e-mail accounts, cloud-based services, social networking platforms, and synchronized desktop applications. The electronic data can contain detailed sequences of events indicative of criminal intent, interrelationships between organized networks of
offenders, and the whereabouts of suspects of criminal activity. A large quantity of electronic evidence (e-evidence) is gathered by various service providers, such as telecommunication services, information society services, the Internet, and cloud services. Compelling service providers to disclose these data requested by law enforcement bodies by means of production orders has recently become a significant building block in (modern) criminal investigations that is still facing the problem of privacy protection laws discussed many years ago by Goemans and Dumortier (2003, p. 161), by Geist (2003), and later within the UN study “Comprehensive study of cybercrime” (Malby et al., 2013).

The information technology today is at the same time the subject (place), the tool (instrument) and the object (target) of crime (Savona & Mignone, 2004). The available technical devices facilitate traditional crimes, such as offences against property and offences causing personal harm (McQuade, 2006, p. 157), but the use of technology in committing cybercrime is much more difficult to address within the existing national legal frameworks (Hughes, 2003), despite the common understanding that crime in the interconnected world is transnational in terms of the physical location of victims, criminal actors and e-evidence. Despite mutual agreements signed between many countries in the world and extra-territorial legal provisions for criminal acts committed in foreign jurisdictions, the practical implementation of the laws enabling provision of e-evidence was assessed as ineffective (Malby et al., 2013).

Whilst an offender may be apprehended in one jurisdiction, the e-evidence required in an investigation may be located in another country (Brown, 2015), and that requires a special legal form to order its handing-over. For most forms of crimes, in particular in cases of cybercrime whose increasing occurrence we witness in the last decade, e-e evidence – such as account subscriber information, traffic or metadata, or content data – has become of ultimate importance as it provides significant leads for investigators, often being the only evidence connected to the crime acts. E-evidence connected to crime acts perpetrated in the interconnected society is often cross-jurisdictional, because often the data is stored outside the sphere of influence of the investigating authority in the country where investigation has been launched, or by providers of electronic communication services and platforms whose main seat is located outside the investigating country, resulting in the fact that investigating authorities are not able to use their domestic investigative tools.

According to Brown (2015), e-evidence should be used in the criminal justice process only when a course of conduct is considered truly criminal and warranting prosecution. Fundamental to most legal systems regarding the applicability of the evidence is the principle that »no matter how harmful the actor’s behaviour or the particular act is«, it cannot be prosecuted unless it is formally prohibited by law (Grabosky, 2007; Tikk, 2011). As a measure of applicability, the following elements must be present for an act to be classified as cyber-based (Brown, 2015, p. 57):

- “The conduct is facilitated by information and communications technology;
- The conduct is motivated by an intent to commit harm against a person or organization;
- The perpetrated or intended harm encompasses conduct amounting to interference or damage to either tangible or intangible property owned by a person or organization; and
• The conduct concerned is criminalized within either the jurisdiction of the victim or the jurisdiction of the accused.”

Under this definition, cybercrime is considered as a subset of conventional crime in which information and communication technology is used as a vehicle or tool to commit traditional criminal offences (Zhigang, 2011). This definition adheres to the rudiments of legal interpretation applied to traditional criminal offence.

A problem with collecting e-evidence is that the investigators must ensure that they abide by applicable laws or otherwise risk that the seized exhibits will be declared inadmissible at trial. In some jurisdictions there are exceptions that may justify warrantless search and seizure activities (e.g. consent, ‘emergency’ terrorist situations, plain view doctrine, search relating to arrest, etc.) The actual search of the data stored on a device usually requires a warrant in common law countries. In circumstances where there is a substantial risk of losing evidence, such as where data sanitizing and other anti-forensics tools are active, some jurisdictions permit law enforcement to perform a limited search of devices without a warrant due to the perceived vulnerability of the data (Dee, 2012). During warrant activities, investigators may also discover legally protected sources of electronically stored information (e.g. the doctrine of legal professional privilege, public-interest immunity, etc.), adding a layer of complexity to the process of evidence handling. Also, many investigators encounter administrative delays in obtaining legal authority to conduct police investigations due to judicial uncertainty.

Another problem is connected to the preservation of stored data. The issue of data retention remains controversial as the EU Data Retention Directive (European Parliament and Council of the European Union, 2006) was declared as invalid due to a violation of the Charter of Fundamental Rights of the European Union (European Parliament, Council of the European Union, and the Commission, 2000) because the Directive exceeded the limits imposed by the principle of proportionality. In addition, the legal treatment of data may differ significantly from one country to another, posing a minefield of technical and legal complexities. As such, it becomes critical that investigators and prosecutors be well informed of geo-specific data-mapping issues including embargoes or prohibitions of data exchange.

As a conclusion, it can be claimed that Law Enforcement Authorities (LEAs) and their territorially restricted investigatory powers face complex and yet un-solved sovereignty questions when compelling service providers to provide data. This is because the respective service provider might either be based abroad, and/or is storing the data sought after outside the investigating state’s territory. Using the official channel of investigation, mutual legal assistance is regarded as burdensome and slow, in particular where the service provider being based abroad or data storage abroad is the only cross-border element of the case. It is therefore not surprising that orders to produce (data) with a cross-border dimension have been causing challenges before the courts in the US and Europe, accompanied by political debates.

This paper presents the current issues and proposes legal remedies for removing barriers to gathering cross-border e-evidence to ensure a more efficient fight against crime and cybercrime. In this context the paper briefly presents the current legal scene in the EU, the efforts related to the adoption and implementation of the European Investigation Order Directive (European Parliament and Council of the European Union, 2014) and
the provision of legal procedures for e-evidence collection proposed within the EU proposal for the Directive for orders to preserve and produce evidence related to criminal acts in a territory different from the location of the crime act (European Parliament and Council of the European Union, 2018a).

This paper is organized as follows: the introduction section presents the problem, the next section provides a brief description of the current legal scene, the third section introduces the reader to the results of the LIVE_FOR project oriented to raise the awareness and the implementation of the EU European Investigation Order Directive among the EU Member States. The last two sections of the paper deal with the procedures proposed in the new EU regulation for collecting e-evidence. The concluding marks provide brief assessments about the expected removals of jurisdiction barriers for a more efficient justice processing of criminal acts in an interconnected world.

The Current Legal Scene and Cross-Border Search for E-Evidence

1. Budapest Cyber Crime Convention

The best-known juridical act in the fight against cybercrime within the interconnected society with an international dimension is the Council of Europe’s Convention on Cybercrime Act (2001). This document is a result of the efforts dedicated to solving the problem of cyber-based crime by the members of the Council of Europe (CoE), Interpol, Europol, the Organization for Economic Cooperation and Development, the G8 Group of States, Commonwealth and the United Nations (UN). The document of the Council of Europe is known as Budapest Cybercrime Convention (hereinafter referred to as the CCC) that entered into force in July 2004. The document was ratified by 43 out of 47 Members (until August 2018) of the Council of Europe (San Marino, Ireland, Russia, and Sweden have not yet ratified it) and by Argentina, Australia, Cabo Verde, Canada, Chile, Costa Rica, the Dominican Republic, Israel, Japan, Mauritius, Morocco, Panama, Paraguay, the Philippines, Senegal, Sri Lanka, Tonga, and the United States of America. The CCC is not limited to matters of cybercrime as the item braces investigatory measures concerning “the collection of evidence in electronic form” for any form of offence where such electronic evidence may be relevant (de Hert et al., 2017). The CCC with its 61 contracting states constitutes the first and most significant multilateral binding instrument to regulate cybercrime, sometimes considered as “the most comprehensive international standard to date” (de Hert et al., 2017).

The implementation of the CCC that required the existence of an MLA (Mutual Legal Assistance) agreement between the signatories has shown that the implementation requires a more detailed description of the specific instrument provided within the CCC – the production order. The answer to this finding was provided in March 2017 by the Cybercrime Convention Committee (hereinafter T-CY) of CoE, in the form of a Guidance Note (Cybercrime Convention Committee, 2017) focused on the interpretation of Article 18 and interpretation of the “Production orders for subscriber information” (hereinafter Guidance Note). Soon after the adoption of the Guidance Note criticism about the interpretation of the article (18) (1) (b) CCC in the Guidance Note appeared regarding the issuing of a production order to a “service provider” as defined in Article 1 (3) of the CCC. This article specifies the service provider as “(a) any public or private entity that provides to users of its service the ability to communicate using a computer
The interpretation of Article 18 (1) of the CCC which defines production orders based on the service provider definition in the Guidance Note, allows the issuance of production orders by Law enforcement bodies to foreign established service providers or persons, without specifying whether the required subscriber information is stored within or outside the ordering state’s territory. According to several experts (de Hert et al., 2017), for legal matters this interpretation is insufficient and misleading because Article 18 (1) (a) CCC is interpreted in the Guidance Note as an additional legal basis for production orders by enabling the search through a whole spectrum of data including subscriber information, traffic and content data stored abroad by a provider that is at the same time physically present within the ordering state’s territory. The exact definition of these types of data and their potential location is not provided in the Guidance Note (de Hert et al., 2017).

Also, the Guidance Note with the provided interpretation is misleading about the way the data should be sought. The Guidance Note claims that the agreement by the cooperating states about the respective document does not allow to be classified as consent to the extraterritorial enforcement of domestic production orders. This statement can be true only in cases when a production order addresses foreign-based service providers storing data on foreign territory. In addition, this action is not considered to be an exercise of state power in the territory of another state. Otherwise, such a production order would require a permissive rule derived from international custom or convention in order to not conflict with international law. The extension of the scope of Article 18 of the CCC in the proposed way by the Guidance Note represents a challenge to the principle of territoriality and sovereignty, which are essentially interconnected with the protection of fundamental rights and the rule of law (Hildebrandt, 2013).

It is also crucial that the CCC and the Guidance Note do not pay any attention to the protection of fundamental human rights and the rule of law as any responsibility in regards to the effective protection of fundamental rights is specified as follows: “the parties to the convention are expected to form a community of trust that respects Article 15 CCC (Cybercrime Convention Committee, 2017). The same document does not clarify what subscriber information actually stands for, although this missing information is of tremendous importance to the evaluation of the impact the point of privacy has on production orders issued according to Article 18 (1) (b) CCC. Another gap in the Guidance Note is the neglected clarification of a dynamic IP address and whether this data can be considered as subscriber information, or does it fall into the category of traffic data and is consequently outside the scope of Article 18 of the CCC. The lack of consistent definitions of different types of data in the Guidance Note may also result in conflicts of law as regards the scope of envisaged measures. This may lead to misunderstandings between the requesting authority and executing authority or the service provider addressed (European Commission, 2017). The extension of the scope of Article 18 of the CCC in the proposed way within the Guidance Note presents a challenge to the principle of territoriality and sovereignty, which are essentially inter-connected with the protection of fundamental rights and the rule of law (Hildebrandt, 2013). It was expected that the Guidance Note’s interpretation of Article 18 CCC would circumvent the established instruments of judicial cooperation, such as the MLA agreements, which allow the
cooperation of Legal Enforcement Agencies from different countries, while ensuring respect for the interest of sovereignty of each country.

2. Directive 2014/41/EU Regarding the European Investigation Order

Another legal document that addresses the collection of e-evidence is the Directive regarding the European Investigation Order in criminal matters (Directive 2014/41/EU, hereinafter the EIOD), adopted by the Parliament and the Council of the European Union on 3 April 2014. From 22 May 2017, the Directive replaced the corresponding provisions of the following conventions applicable between the Member States bound by this Directive (Art. 34 of the EIOD):

a) the European Convention on Mutual Assistance in Criminal Matters of the Council of Europe of April 1959, as well as two additional protocols, and bilateral agreements concluded pursuant to article 26 thereof;

b) the Convention implementing the Schengen Agreement; and


In addition, the EIOD replaces the Council Framework Decision 2008/978/JHA on the European Evidence Warrant to obtain objects, documents and data to be used in proceedings in criminal matters and it also replaces those provisions of the Framework decision 2003/577/JHA regarding the freezing of evidence (the recitals 25 and 26 of the EIOD).

As of 2019 all EU member states but two have adopted the Directive. Denmark and Ireland opted out from its adoption and as a result will continue to use Mutual Legal Assistance Treaties (hereinafter MLATs) to carry out judicial cooperation. The EIOD aims to overcome the complexity and fragmentation, which the system of mutual legal assistance represents. It is supposed to do so by replacing with a single instrument the different rules and systems for obtaining all kinds of evidence.

The European Investigation Order (EIO) is “a judicial decision which has been issued or validated by a judicial authority of a Member State (“the issuing state”) to have one or several specific investigative measure(s) carried out in another member state (“the executing state”) to obtain evidence in accordance with this Directive” (European Parliament and Council of the European Union, 2014).

Regarding the authorities capable of issuing and validating an EIO (Article 2(2)), the EIOD provides details on the meaning and scope of the term “judicial authority” and lists the following entities: judges, courts, investigation judges, and public prosecutors competent in the crime case concerned. While based on the principle of mutual recognition, the EIO also incorporates the flexibility of the traditional system of MLAT (Recital 6 of the EIOD) and thus the executing states enjoy the margin of manoeuvre when receiving a request via an EIO. The EIOD applies to any investigative measures directed to the gathering of any type of evidence, including e-evidence, in criminal proceedings, except in the case of joint investigation teams (Article 3 of the EIOD).

The Directive provides specific rules for e-evidence in two cases:

- Requests for the identification of persons holding a subscription of a specified phone number or IP addresses (Article 10 (2)e of the EIOD).
- Requests for the interception of telecommunications (Article 30 of the EIOD).
The EIOE defines the deadlines for the executing authority to decide on the recognition or execution of an EIO and an additional time limit to carry out the investigation measure. By criminal proceedings, the EIOE refers to those that are initiated by judicial and administrative authorities. In case of the latter, this will only apply insofar they give rise to proceedings before courts with criminal jurisdiction (Article 4 of the EIOE).

Other instruments of judicial cooperation adopted in the EU with the exception of the EU Decision 2003/557JHA on the execution of orders for freezing property or evidence do not consider or mention the term of e-evidence. E-evidence is mentioned only as an instrument that refers to the preservation of existing evidence without any reference to the production of e-evidence found on cyber devices and networks. The classification of electronic data is provided in Article 5 of the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communication services or of public communication networks as the traffic data and content data defined as categories of data to be retained. However, the Directive on data retention was annulled in 2014 because it did not comply with the legal obligations arising from the Convention on the processing of personal data and the European Convention on the protection of human rights and fundamental freedoms.

3. Direct Cooperation with Service Providers

National criminal courts are not bound to the definitions offered in the EU directives. So, the cooperation is left to the system applied in a particular country and the service providers. Member States have different approaches when it comes to considering the obligation of service providers established in another country to comply with a request carried by their own national authorities:

- **Voluntary:** Austria, Romania, Sweden, Hungary, Netherlands, Greece, Czech Republic, Denmark, Finland, Slovenia, Italy, Estonia, Luxembourg, Malta, Bulgaria.
- **Mandatory:** Belgium, Cyprus, Spain, Portugal, United Kingdom, France, Lithuania.

When data is requested under an EIO or MLAT’s instruments, the communication is carried out between two public authorities, while in case of a direct cooperation with foreign service providers the dialogue is between a public and a private entity. As a result, the private parties’ obligations concerning deadlines, the form of execution or confidentiality differ. It is also worth noting that a great number of member states do not provide a legal basis for service providers established in their territory to respond to direct requests of law enforcement. To remedy the situation, the European Commission’s recently proposed the Directive about the appointment of legal representatives for the purpose of enabling the collection of e-evidence in criminal proceedings (European Parliament and Council of the European Union, 2018b) that offers a structured description of service providers in the context of criminal investigations. In that regard, article 2(2) of the Directive proposal defines a service provider as any natural or legal person that provides one or more categories of services:
Electronic communication services: the definition distinguishes between providers of three types of services: Internet access service, interpersonal communications service, services consisting wholly or mainly in the conveyance of signals, including telecommunications services such as transmission services in networks used for the provision of machine-to-machine services and broadcasting.

Providers of information society services embrace “any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services”, for which the storage of data is a defining component of the service provided to the user such as social networks, online marketplaces and other hosting service providers (Article 2 (2)b of the Directive proposal).

Providers of names and numbering services for the internet such as IP addresses, domain name registries, domain name registrars and related privacy and proxy services (Article 2 (2)c of the Directive proposal).

**LIVE FOR Surveys and Findings**

The adoption of the Directive 2014/41/EU regarding the European Investigation Order (EIO) in criminal matters is considered a milestone for judicial cooperation in criminal matters in the European Union. The time frame for the adoption in the national legislative systems was by 22 May 2017. As the matter treated in the Directive was new and raised several questions regarding the implementation especially when it comes to collecting e-evidence in an interconnected world, the two-year LIVE _FOR project from the EU JUST-2015-JCOO-AG program was launched with the following major goals:

- to identify the state of the art, problems and obstacles in relation with the implementation of Directive 2014/41/EU and the EIO, and
- to raise the awareness among executive authorities about the newest scientific and educational achievements in the selected domains (live forensics in cloud computing environments).

The project agenda is based on several instruments designed to meet the project objectives. It was clear at the starting date of the project in 2016 that there were juridical authorities that leverage the technical subject matter when building a case, however the need was also acknowledged for continuing the professional development by means of courses that directly address the impact of information technology upon the modes of criminal offences, with a focus on data for fraud, corruption, and data-driven acts causing personal harm. The awareness of the digital forensics discipline and characteristics of electronic evidence was also considered to be part of the required and ongoing training. It was common understanding that it is incumbent for judges to have a comprehensive understanding of the collected material before they approach a crime case. In that context, the following instruments were envisaged in LIVE_FOR:

- Identify the state of the art in relation with the implementation of Directive 2014/41/EU within the EU MS and the problems that hinder the implementation and adoption of EIO in the MS legislative order, especially regarding the
differences between the judicial systems of EU MS and how this influences the implementation of the EIO;

- Identify the level of awareness among executive authorities about the approaches required for investigation and collection of e-evidence in a networking environment with a task for increasing the awareness of executive authorities about EIO mechanisms and the digital forensic methods for investigation in cloud computing environments;
- Identify the needs for mutual learning and exchanging best practices among the target groups regarding subjects covered by LIVE_FOR;
- Prepare training workshops and inputs for the new curricula and educational subjects that will increase the competence of executive authorities in relation with the use of the EIO.

In implementing the first instrument, two joint meetings of the target community consisting of judges, public prosecutors, and investigative judges were organized in 2017, one in Brussels for the participants from the Western EU countries and the other one in Ljubljana focused more on the participants coming from Central Europe. Both joint meetings used a similar format including keynote presentations, panels, and group discussions. In total, 53 participants from 18 countries attended the meetings, 26 participants were either prosecutors, judges or investigators, 5 participants were policymakers, 7 participants were academics, and 15 participants were LIVE_FOR project partners and advisory board members.

The prosecutors and the judges welcomed the European Investigation Order and expressed a generally positive opinion about the Directive at the meetings. However, the usefulness of the EIO was not strictly confirmed by the participants, some of them found that the EIO was useful because of its simplicity, for the others this instrument did not look very useful. The panels at the joint meetings stressed especially on the need for (cross-border) remote e-evidence searches as well as for unilaterally prepared data requests to the foreign service providers. In this context, a potential amendment to the EIO was discussed regarding the unilateral interception of electronic communications according to Article 31 of the EIOD. Concealed measures were discussed and were identified as an EIO problem because they differ in each of the EU MS. The legal use of the e-evidence found abroad may be treated differently from country to country, somewhere it is legal and accepted by the court, in some other countries it is not accepted in justice processes. Several comments were also issued regarding the definition of privilege (Article 11) that needs a more exact definition.

Similarly, the definition of the content of e-evidence is not exactly specified; as an example, the subscriber identification was pointed out as a not sufficiently clearly defined item (are the required subscriber data their name and surname, or name, surname, and date of birth, or also their permanent residence, copy of contract, billing info, etc). These data change over the time, and they are not always available. The invalidation of the Data Retention Directive was commented with mixed feelings as the time limits for data collection affects the collaboration of the collaborating parties. On the one hand, the limits set in the EIOD ensure that the requests are executed on time, but they might as well prolong the time of collecting the evidence, as the executing authorities might in some
cases wait until the deadline passes. Data encryption was also raised as a problem that prevents an understanding of the content.

Both meetings stressed that training on e-evidence and EIO is much needed but should be provided in a simplified form and on a national level in national languages. It should be based on (real) case studies and practiced among prosecutors/judges in a face-to-face setting. A request was also expressed for the legal experts and technical experts to cooperate in order to align the efforts in establishing a common framework for understanding the related EIO issues and introducing a common terminology, tools and practices used by the two in solving the same problem that has two aspects: a legal and a technical one. Another request addressed the provision of guidelines for collecting e-evidence from the United States to be prepared by the European Commission as most of the data is stored overseas and not in Europe. The participants also suggested information about the Member State’s own (EIO) contact point in the national language as well as a best-practice guide for the use of the EIO as a help for less experienced prosecutors/judges to be set.

The second instrument was an online survey, in which 150 people from 20 countries participated, among them 45.3% were public prosecutors, 29.3% were judges, 4.0% investigation judges, 4.0% representatives from Ministries of justice, and the rest from law enforcement and other institutions. The survey was designed as an online questionnaire with a goal to study the awareness about the Directive 2014/41/EU and the EIO, the practices on cross-border evidence collection, and educational and training needs in this field. The survey was anonymous, ensuring that the participants could share their honest opinions. However, for those interested, the form offered the possibility of sharing a contact address. The questionnaire was structured in four parts: Socio-demographics, Directive 2014/41/EU and European Investigation Order, Procedures, and Educational and training needs. The questions were available in English, Slovenian, and Spanish. The online survey was available for completion from 11 April 2017 to 26 September 2017.

Even though the Directive and the EIO are new instruments and not widely implemented and adopted yet in the EU member states in 2017, most of the respondents were aware of them. Out of 108 survey participants who answered this question, 66 knew about the Directive and EIO. The highest awareness rate was found among the investigative judges and public prosecutors. A minority of the respondents (25.8%) expected or faced obstacles in implementing the Directive. The obstacles mentioned include a parallel use of freezing orders, a lack of funding to prepare IT systems for the new requirements, a lack of training and legal advice on when and with which countries to use EIO, an unclear definition of the suspect status, Brexit, resistance to changes, and judicial cooperation between countries that have already implemented the Directive and those that have not. The most frequently mentioned problem expected in the future was a difference in the national legislations that implement the EIO. A minority of the respondents are involved in investigation cases that require digital evidence to be collected outside their country on a weekly (13.9%) or on a monthly basis (9.7%). They also stated that in this type of cases they face primarily legal challenges, but also a lack of understanding due to different systems and cultures, and a lack of knowledge in some technical areas. Help from technically skilled people is asked in the country of case investigation. 46.3% of the participants indicated their level of knowledge in the field of digital investigation is low while for 44.8% it is close to medium; almost all (97%) felt that their current knowledge of digital investigation needed upgrading. The details of the
questionnaire including the questions, processed data, and details about the knowledge skills and competencies needed for a successful cross-border digital investigation and the EIO preparation can be found on the LIVE_FOR web page in the Deliverable 2.1 (Klobučar et al., 2017), URL: http://www.live-for.eu/. The educational and training topics (representing a particular group of topics) of interest for the participants are presented in Fig. 1.

**Figure 1 Selected educational and training topics**

Based on the results of the two instruments, the project team of LIVE_FOR had prepared the curriculum for several webinars and two face-to-face training workshops that were held in 2018.

**Proposed EU Regulation on Production and Preservation Orders – Do the New Instruments provide answers to the Identified Problems and Drawbacks?**

### 1. The Current Legal Framework

The current legal framework for cross-border access to evidence with bilateral and multilateral mutual legal assistance (MLA) instruments was replaced in the EU on 22 May 2017 by the European Investigation Order (EIO). According to the EIO national regimes of the EU Member States and third countries, cross-border access to electronic evidence may be obtained in three ways:

- through formal cooperation channels between the relevant authorities of two countries, usually through MLA/EIO (where applicable), or police-to-police cooperation;
through direct cooperation between law enforcement authorities of one country and service providers whose main seat is in another country, either on a voluntary or mandatory basis; notably service providers established in the United States (U.S.) and Ireland reply directly to requests from foreign law enforcement authorities on a voluntary basis, as far as the requests concern non-content data;

through direct access from a computer, as allowed by some Member States’ national law.

Several experts have found these possibilities for gathering cross-border evidence especially in case of cyber space insufficient and inefficient (de Hert et al., 2017). Many juridical authorities and the expert community as well the Council of the European Union, in its efforts to improve criminal justice in cyberspace, have come to the conclusion that the European Commission should “explore the possibilities for a common EU approach on enforcement jurisdiction in cyberspace in situations where existing frameworks are not sufficient, for example in situations where relevant e-evidence moves between jurisdictions in short fractions of time” (Council of the European Union, 2016).

The Commission was specially requested to determine “which connecting factors can provide grounds for enforcement jurisdiction in cyberspace” and “whether, and if so, which investigative measures can be used regardless of physical borders” (Council of the European Union, 2016). Similar concerns were expressed especially in relation to the MLAT process and its reform by the US Department of Justice set up in the document “Cross-Border Law Enforcement Demands: The analysis of the US Department of Justice’s Proposed Bill” was issued on August 2016. The answer to these requests came on 17 April 2018 in the form of two documents: The Impact Assessment about the Proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and the Proposal for a Directive laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (European Commission, 2018). The latter document is proposed as a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (the Regulation).

The main objective of the Regulation is setting an EU legal framework for investigative measures addressed to a service provider enabling authorities to request ("production request") or order ("production order") a service provider in another Member State to disclose information about a user. However, the proposed Regulation is much more comprehensive and detailed. The proposal targets the specific problem created by the volatile nature of electronic evidence and its international dimension. It seeks to adapt cooperation mechanisms to the digital age, providing judiciary and law enforcement tools to address the way criminals communicate today, and to counter modern forms of criminality.

The use of such tools depends on their being subject to strong protection mechanisms for fundamental rights. This proposal improves the legal certainty for authorities, service providers and persons affected, and maintain a high standard for law enforcement requests, thus ensuring the protection of fundamental rights, transparency, and accountability. The suggested instrument is designed to co-exist with the current judicial cooperation instruments, e.g. the CCC and EIO, as they are considered relevant and can be used as appropriate by the competent authorities.
This applies as well to bilateral agreements between the Union and non-EU countries, such as the Agreement on Mutual Legal Assistance (‘MLA’) between the EU and the US and the Agreement on MLA between the EU and Japan. Similar agreements are expected to be signed with other countries as well. The EIO Directive, which has to a large extent replaced the Convention on Mutual Assistance in Criminal Matters, covers any investigative measure including e-evidence – but as mentioned in Section 3 above, the EIOD does not contain any specific provisions on this type of evidence. So, the proposed instruments in the Regulation are not intended to replace the EIO for obtaining e-evidence, but are prepared as an additional tool for authorities that allow much more freedom in the search for e-evidence. An authority in a country where the addressee of the Production 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; however, robust safeguards and provisions, such as the validation by a judicial authority in each case, are provided in the legal framework of the regulation.

2. Instruments and Mechanisms Designed in the Proposed Regulation

The proposed regulation is a document organized in five chapters and 25 sub-chapters presented on 55 pages. The preparation of the mechanisms in the new Regulation was based on a consultation with relevant stakeholders that lasted for over a year and a half, to identify problems related to cross-border electronic evidence collection and preparation of instruments and mechanisms for going forward. This was done through surveys, ranging from open public consultations to targeted surveys with relevant public authorities. Group expert meetings and bilateral meetings were also organised to discuss the potential effects of the EU legislation. Conferences discussing cross-border access to electronic evidence were used to gather feedback on the initiative.

These activities resulted in the proposed Regulation which is expected to be adopted soon as an EU Directive and to become part of the Union legal framework. The main objectives of the proposed Regulation are to reduce delays in cross-border access to e-evidence, to ensure cross-border access to e-evidence where it is currently missing, and to improve legal certainty, the protection of fundamental rights, transparency, and accountability.

The main instrument to achieve these objectives are the instruments and aligned mechanisms for issuing production and preservation orders. The regulation sees the production order as an action issued to seek the preservation or production of data stored by a service provider located in another jurisdiction that is required as evidence in a criminal investigation or criminal proceedings. Such orders may only be issued if a similar measure is available for the same criminal offence in a comparable domestic situation in the issuing State. Both orders 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. The orders refer to the specific known or unknown perpetrators of a criminal offence that has already taken place. The European preservation order only allows preserving data that is 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.
The proposed Regulation and the exhaustive accompanying document about its impact (European Commission, 2018) describe how the proposed instruments will help in overcoming most of the identified problems in the area of cross-border e-evidence collection in cases of criminal acts:

a) Provision of better applicability of collected cross-border e-evidence at trial due to the applicability of the regulation to Member States and envisaged agreements with third countries (e.g. the US) with different jurisdictions. The proposed Regulation defines the scope in Article 1 of the document. The Article 82(1) of the Treaty on the Functioning of the European Union ensures the mutual recognition of judicial decisions by which a judicial authority in the issuing Member State addresses a legal person in another Member State and even imposes obligations on it, without prior intervention of the judicial authority in that other Member State. The European Production or Preservation Order enables the intervention of a judicial authority of the executing state when necessary to enforce the decision. The proposed regulation is designed to be directly applicable as it provides clarity and greater legal certainty and avoids divergent interpretations in the Member States and other transposition problems that the Framework Decisions on the mutual recognition of judgments and judicial decisions have encountered. Given the diversity of legal approaches, the number of policy areas concerned (security, fundamental rights including procedural rights and protection of personal data, economic issues), and the large range of stakeholders, the proposed Regulation at the Union level promises to provide the most appropriate mechanisms to address the identified problems.

Regarding third countries, for example the US, specific policy measures are envisaged. International agreements coherent with EU-internal solutions could be set to provide a basis for closer international cooperation with safeguards comparable to those of the EU-internal solution with regard to individuals' rights, including judicial redress. These agreements could cover judicial cooperation, direct cooperation and/or direct access.

b) The exact definition of the entity that can issue a production order for collecting e-evidence is presented in Article 4, while the condition for issuing orders are specified in Article 5. The proposed Regulation introduces binding European Production and Preservation Orders that need to be issued or validated by a judicial authority of a Member State. The European Production Order is implemented by issuing a European Production Order Certificate (defined in Article 8), which is translated and sent to the service provider. An order can be issued to seek the preservation or production of data stored by a service provider located in another jurisdiction and required as evidence in criminal investigations or criminal proceedings. Such orders may only be issued if a similar measure is available for the same criminal offence in a comparable domestic situation in the issuing state. The misleading approach in the Guidance Note about the method to look for the data as it claims that agreement by the party states to the respective document will not be classified as consent to extraterritorial enforcement of domestic production orders, is clearly set in the Regulation and explained in the Impact assessment document. Article 2 defines the Member States and authorities that could be involved in the procedure. A definition of the issuing authority is included in Article 4. A judicial authority always needs to be involved as either an issuing or a validating authority. For orders to produce transactional and content data, a judge or court is required. For subscriber or access data, this can also be done by a prosecutor.
c) The category of data that could be searched for in a production order for collecting crime related e-evidence. The Guidance Note of the CCC allows for a whole spectrum of data, such as subscriber information, traffic and content data stored abroad by a provider that is physically present within the ordering state’s territory. However, the exact definition of these types of data and their potential location is missing in the Guidance Note. The proposed regulation relies on a specification of data that can be obtained by means of a European Production Order by the competent authorities on the definition of electronic communication services defined in the proposal for a Directive establishing the European Electronic Communications Code (European Commission, 2018). They include subscriber data, access data, transactional data (the three categories commonly referred to jointly as ‘non-content data’), and stored content data. They are defined as follows:

- **Non-content data:**
  - Subscriber data, which allows the identification of a subscriber to a service. Examples: subscriber’s name, address, telephone number.
  - Metadata, which relates to the provision of services and includes “electronic communication metadata”, as defined in the e-Privacy proposal (European Parliament and Council of the European Union, 2017). Examples: data relative to the connection, traffic or location of the communication.
  - Access logs, which record the time and date an individual has accessed a service, and the IP address from which the service was accessed;
  - Transaction logs, which identify products or services an individual has obtained from a provider or a third party (e.g. purchase of cloud storage space).
  - Content data. Examples: text, voice, videos, images, and sound stored in a digital format, other than subscriber or metadata.

The type of data defined above may imply a different treatment by existing rules and different procedures to access it. Each of the above categories may contain personal data and are thus covered by the safeguards under the EU data protection acquis, but the intensity of the impact on fundamental rights varies between them, in particular between subscriber data on the one hand and metadata and content data on the other. All the data specified above refers to electronically stored data that already exists. Intercepted data (i.e. data from the real-time interception of telecommunications) is out of the scope of the proposed Regulation as there are specific and significantly different rules that determine access to that data.

However, it should be noticed here that the proposal limits the instruments to collect only data that are necessary to achieve its main objectives. In particular, the proposal is limited to requests for stored data (data from real-time interception of telecommunications is not covered) and to orders issued in criminal proceedings for a specific criminal offence under investigation. It therefore does not cover crime prevention or other types of proceedings or infringements (such as administrative proceedings for infringements of the rules of law) and does not require providers to systematically collect or store more data than they do for business reasons or compliance with other legal requirements.
In addition to the specification of the category of data, the proposed Regulation addresses providers of the following services:

- The revised definition of electronic communications services covers both traditional telecommunication services (example: voice telephony, SMS, internet access service) as well as new Internet-based services enabling inter-personal communications, such as voice over IP, instant messaging and web-based email services (Over-the-Top communications services, 'OTTs'). These OTTs are in general not subject to the current EU electronic communications framework (i.e. Directive 2002/21/EC), including the current e-Privacy Directive, which in general applies only to traditional telecommunication services. In line with the expansion of the EU electronic communications and ePrivacy framework, OTTs should be covered by this initiative as well (e.g. Gmail, WhatsApp);
- Information society services as defined in the Directive 98/34/EC that store data at the individual request of a recipient of a service; this includes a variety of known services providers such as social networks (e.g. Facebook and Twitter), cloud services (e.g. Microsoft, Dropbox or Amazon Web Services), online marketplaces (e.g. eBay or Amazon marketplace) or other hosting service providers (e.g. Bluehost);
- Internet infrastructure services such as IP address providers and domain name registries and registrars and associated privacy and proxy services (e.g. GoDaddy) (European Commission 2018).

d) The issue of human rights protection is addressed in Article 1(2) by a statement that clearly stresses that the Regulation shall not have the effect of modifying the obligation to respect the fundamental rights and legal principles as enshrined in Article 6 of the Treaty on the European Union. This addresses the categories of data that contain personal data and are covered by the safeguards under the EU data protection acquis. The impact of the Regulation on the fundamental rights varies, in particular between subscriber data on the one hand and transactional and content data on the other hand. It is essential that all these data categories are covered by the Regulation instrument: subscriber and access data are the starting point to obtain leads in an investigation about the identity of a suspect and will be protected according to the EU data protection acquis as specified in the introductory chapter of the Regulation: “Personal data covered by this proposal is protected and may only be processed in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Directive for Police and Criminal Justice Authorities (Law Enforcement Data Protection Directive).” The GDPR (European Parliament and Council of the European Union, 2016a) entered into application for the EU members on 25 May 2018, while the Law Enforcement Data Protection Directive (European Parliament and Council of the European Union, 2016b) was transposed by the Member States by 6 May 2018.
e) The cooperation of national criminal courts is regulated with the system applied in a particular country and the service providers. Additional policy measures are proposed to cover this problem:
The Impact assessment document of the Regulation proposes the creation of single points of contact, both on the public authorities’ side and on the service providers’ side. On the public authorities’ side in the Member States, it could significantly improve the direct cooperation between those authorities and service providers by e.g. ensuring the quality of outgoing requests and building relationships of confidence with providers, as they know their counterpart. On the service provider's side, the proposed creation of a single point of entry could also improve the direct cooperation between those authorities and service providers, for example by helping to clarify the provider’s policies. Another proposed measure is the standardisation and reduction of forms used by law enforcement, while judicial authorities could facilitate the creation of requests by law enforcement and increase the confidence of service providers when it comes to the identification of authorities and proper forms used.

Regarding the cooperation with the US practical measures for enhancing the judicial cooperation between public authorities in the EU and the US, the Impact assessment document envisages the following procedures based on the existing mutual legal assistance: regular technical dialogues with the US Department of Justice to continue to improve the process, speed and success rate of MLA requests, and maintaining regular contacts between the EU Delegation to the US, the Commission and liaison magistrates of Member States in the US to discuss MLA process issues. In addition, the US Department of Justice’s Proposed Bill and the Cross-Border Law Enforcement will be analysed and followed according to the proposer’s request. These issues are explained in the introductory part of the Regulation by clarifying the complementarity between different measures (in particular the EIO Directive, negotiations of an additional protocol to the Budapest Convention and the joint review of the EU-US MLA Agreement) regarding the timing and depth, and the baseline scenario and its developments that are likely to occur independently from the adoption of the proposed measures.

The problem of education and training. The provision of opportunities to exchange best practices and for training of public authorities in the EU on the cooperation with US-based providers is envisaged, as well as additional trainings for law enforcement and judicial authorities to support the functioning of the direct cooperation between judicial authorities and service providers. The training is envisaged not as fragmented per country, but rather as centralised to ensure for synergies. It should be based on the EU Partnership Instrument for improving cooperation. Funds are provided for this activity. Additionally, an online information and support portal is planned at the EU level to provide support to investigations, including information on applicable rules and procedures. The platform could have a form of a static repository for service provider policies, but can also be used as an interactive tool guiding law enforcement authorities in the identification of the relevant service provider and appropriate channels to be used, and for creating and submitting requests to several service providers.

Discussion and Conclusion

The new proposed Regulation and the cross-border dimension of the problems certainly require the measures and the instruments included in the proposal to be adopted at the EU level in order to achieve the objectives. Most important in meeting the scope of the Regulation in addition to the basic objectives are the agreements for cooperation with
third countries presented in the Impact assessment document. The crimes for which
electronic evidence exists frequently involve situations where the infrastructure in which
the electronic evidence is stored and the service provider running the infrastructure are
under a different national legal framework, within the European Union or beyond, from
the national legal framework of the victim and perpetrator of the crime. As a result, it can
be very time-consuming and challenging for the competent country to effectively access
electronic evidence across borders without common rules proposed in the Regulation. In
particular, Member States acting alone would have difficulty addressing the following
issues:

• Fragmentation of legal frameworks in Member States, which was identified as a
  major challenge by service providers seeking to comply with requests based on
different national laws;
• A better expediency of judicial cooperation based on the existing Union
  legislation, notably via the EIO.

Considering the above issues and the diversity of legal approaches, the number of
policy areas concerned (security, fundamental rights including procedural rights and the
protection of personal data, economic issues), and the large range of stakeholders, EU-
level legislation such as the proposed Regulation is the most appropriate method to
address the identified problems. The proposed Regulation, the practical instruments,
mechanism and policy measures as presented in the Impact assessment document are
elaborated in details and are convincing. They certainly improve the effectiveness of
criminal investigations in the current interconnected society. However, time will be
needed for the measures and the instruments to be adopted and applied.

The development and promotion of national, regional, and international police
organisations related to collecting electronic evidence, including improving national,
regional and international coordination between law enforcement agencies, is progressing
in the recent years, but the more complete instruments and mechanisms are certainly
provided by the proposed Regulation for production and preservation orders for
electronic evidence prepared by the European Commission.

The approach provided by the proposed regulation is substantial, but the vast network
of international telecommunications systems which facilitate cross-border cybercrime
offences demands a common universal framework that is not just regionally centred or
organizationally exclusive. The EU legislation covers only 28 countries. Ideally, this
should take the form of a binding legal instrument, such as a convention on cybercrime
under the auspices of the United Nations. The Budapest Convention is a good example,
as it has been ratified by non-EU member states, but is nonetheless the product of a
regional organization and based mostly on premises and conditions of CoE members.
Contrastingly, a United Nations convention would be considered a joint product of 193
member states, and arguably would offer a broader appeal to the international community,
thereby limiting the safe harbour for cybercrime offenders.

**Acknowledgements**

This work was co-funded by the European Union’s Justice Programme (2014–2020)
through the L I V E _ _ F O R (Criminal Justice Access to Digital Evidences in the Cloud –
L I V E _ F O R en sics) project and by Slovenian Research Agency.
References


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.


