# DIGITAL EVIDENCE AND CRIMINAL LAW COOPERATION IN THE DIGITAL AGE

**Jelena Kostić, LLD**[1]
Institute of Comparative Law, Belgrade, Serbia
**Nataša Mrvić Petrović, LLD**[2]
Institute of Comparative Law, Belgrade, Serbia

**Abstract:** Perpetrators of crimes, especially those that can be classified as economic crime, use various means to cover up the commission of crimes. These means include the use of information technologies, and many of these crimes are difficult to prove without special knowledge. Due to that, the detection and proving of these criminal acts is extremely difficult.

During the pandemic caused by the SARS-CoV-2 virus, there was a great need for the use of electronic evidence in criminal proceedings. Therefore, in an official communication, the European Commission addressed the European Parliament, the European Social Council and the Committee of the Regions by submitting a document on digitalization at the level of the European Union which offered recommendations for overcoming the identified problems.

In this paper the authors started from the assumption that the national legislation of the Republic of Serbia needs to be further improved to be able to use electronic evidence at the national level and during criminal cooperation at the international level. The authors' conclusions are based on an analysis of international regulations, EU documents and national legislation.

**Keywords:** digital evidence, criminal law cooperation, digital age, national level, EU level.

## INTRODUCTION

Issues of electronic evidence and international cooperation in the digital environment are connected by the need to effectively prevent and prosecute high-tech crime,[3] but also any other form of organized

1 j.kostic@iup.rs
2 n.mrvic@iup.rs

3 Cybercrime or computer crime is any form of criminal behavior in the cyber environment in which computer networks appear as means, citation, evidence or environment of a committed crime. Importance of cy-

and individual criminal activity in which information technology is used. The importance of using electronic or digital evidence[4] in a digital environment is growing. In practice, the need for submitting printed records is reduced, the hearing from the digital recording is enabled, and the procedure itself becomes faster and cheaper. This contributes to strengthening the trust of citizens in the judicial system, and thus strengthening the rule of law. Hence the need to examine whether the national normative framework enables adequate implementation of international standards related to the establishment of cross-border cooperation in criminal matters.

The competent authorities in Serbia, in accordance with national regulations, are involved in all forms of organized international cooperation in relation to organized and high-tech crime, based on ratified conventions (Law on Ratification of the United Nations Convention against Transnational Organized Crime and Additional Protocols[5], Official Gazette SRY, 6/2001, Law on Ratification of the Convention on High-Tech Crime[6], Official Gazette RS, 19/2009). In the Ministry of Interior and the judicial system of the Republic of Serbia, there are special bodies responsible for the prevention of and combating high-tech crime (Law on Organization and Competences of State Bodies for Combating High-Tech Crime – ZODOVK, Official Gazette RS, 61/2005). Following the amendment of the law in 2009, various procedures were established to identify, collect and evaluate evidence. However, the lack of financial resources for the procurement and maintenance of a single electronic data exchange system may prevent it from being established. On the other hand, older and insecure systems that are used are more exposed to the risk of cyber threats, which calls into question the integrity of digital data that can serve as evidence in criminal proceedings. A particular obstacle to the use of electronic evidence may be the different levels of knowledge and technical skills of civil servants working in prosecution institutions and the judiciary.

Given that transnational crime is increasingly taking advantage of information technology,[7] legislative solutions are being prepared at the European Union (EU) level to enable the smooth and rapid flow of electronic evidence for law enforcement and courts, especially for the exchange of information between public prosecutors and judges. From a legal point of view, it is necessary to set standards by which evidence gathered in one country via digital tools could be used in other jurisdictions. In accordance with the provisions of CETS 185, an initiative has been launched to strengthen direct private-law cross-border cooperation. Therefore, in the Communication of 2 December 2020 (EC COM (2020) 710 final) the European Commission (EC) expressed the need to accelerate digitalisation in EU

bercrime, especialy via the internet, has grown with the use of computeres in economy, entertainment and government. Cybercrime includes computer crimes as well as computer-related crimes and crimes committed by illegal use of the internet, which may become organized (form of not-traditional organised crime) and evolve into the online criminality (Tropina, 2012: 159–160).

4 They are important because they do not refer exclusively to crimes in the field of high-tech crime, but also to all other crimes that can be committed using information technology.

5 UN Convention (UNTOC) adopted by General Assembly Resolution 55/25 of 15 November 2000, entered into force in 2003.

6 CoE, Convention on Cybercrime (CETS No. 185), Budapest, 23 November 2001.

7 At the end of the 20th century, the phenomenon of cyber-assisted crime was noticed, i.e. traditional organized crime that "moves" into cyberspace and becomes more efficient due to the use of computers in the digital environment, while, on the other hand, organized groups for high-tech crime are emerging (Tropinov, 2012: 159). This trend is a consequence of the hedonistic calculation of perpetrators: according to Depauw (2018) – dealing with organized crime is economically extremely profitable, but there are high risks to the physical integrity of perpetrators, while in high-tech crime there are significantly lower investments but low risks to physical integrity. and that is why criminal activity brings practically the same, if not greater, illegal property benefit to the perpetrator.

space, estimating that there is an uneven use of information and communication tools in the member states.[8]

The latest EU initiatives are a reason to reconsider whether it is necessary in the Republic of Serbia to improve the system of collection, storage and processing of electronic evidence and to make additional efforts in order to bring these procedures in line with international standards. The assumption is that there is a need for this in our law and practice. The authors will prove this by analyzing the provisions of international legal acts, national regulations and initiatives of EU institutions.

## INTERNATIONAL REGULATION

Cybercriminals, who steal from internet users and companies, use hacking infrastructure and hosting to commit crimes. Criminal organizations also use the "bulletproof hosting" infrastructure as protection against cyber threats from the competition (for example, DDoS Protection Service). Moreover, this infrastructure is the basis of their entire "business" model. Illicit trade in goods and services, as well as laundering of money gained from crime, take place with the use of cryptocurrencies and the advantages of numerous small transactions ("micro-laundering").[9] Given that cyberspace is becoming an area for committing crimes in the field of both organized and high-tech crime, it is necessary to analyze the provisions of international acts intended for their prevention. Of particular importance are the UNTOC (United Nations Convention against Transnational Organized Crime) and CETS 185 (Convention on Cybercrime).

The UNTOC was adopted to enhance international cooperation in the prevention of certain transnationally organized criminal activities, the description of which indicates a possible link between computer and organized crime. The signatories are obliged to improve their legislation by prescribing criminal offenses in the field of transnational organized crime (money laundering, corruption offenses, drug trafficking, human trafficking, etc.), to provide for punishment for preparatory actions (agreement to commit a criminal offense or organize a criminal group) and stricter sanctions for the activities of organized criminal groups. The Article 6 of the UNTOC emphasizes the importance of finding, seizing and confiscating proceeds of organized crime and the need to provide for the widest possible range of predicate offenses in national legislations, while Article 7 prescribes the obligations of the signatory states regarding the prevention of money laundering and emphasizes the need to establish mutual cooperation of institutions and efficient exchange of information at the national and international level. In modern conditions, illegal activities to conceal the origin of property acquired through crime imply the use of information and communication technologies, and the application of these technologies is important for cooperation in their detection. Therefore, in every institution, as well as

8 Digitization of the administrative and judicial system is becoming an imperative for successful cooperation at the national and international level in criminal matters. The needs and requirements of the competent authorities must be in line with the obligation to respect the rights of defendants to a fair trial and fair trial (Art. 47 of the Charter of Fundamental Rights, 2016) and the protection of personal data under the General Data Protection Regulation, 2016.

9 Europol (2018) reports that cyber-organized criminals use semi-automated cryptocurrency exchange and decentralized (peer-to-peer) exchange for money laundering that do not require user identification and verification. The COVID-19 pandemic has intensified criminal activities "from the shadows": the Europol report for 2020 states that a large number of smaller short-lived markets have been replaced by large "dark" web markets (Europol, 2020: 56), which is confirmed by information from January 2021 that DarkMarket, the world's largest illegal web market, was closed (Press Release, 2021, January 12).

at the national level, there should be adequate technical equipment and staff who have the appropriate technical knowledge. The Article 18 of the UNTOC regulates mutual legal assistance in investigation, prosecution or judicial proceedings, which is established upon the request of the requesting state, and is realized in accordance with the law, international treaty, agreement or arrangement. It is exceptionally possible for the competent authorities of the states concerned to exchange information directly, provided that they do not thereby infringe national laws (Article 18, paragraphs 4 and 5). If the states have not concluded an agreement, the cooperation shall take place, in accordance with paragraph 13, through the central bodies, authorized to receive requests for mutual legal assistance. In that case, prolongation may prevent timely collection of evidence and timely exchange of information between the competent authorities of the signatory states, and thus means effective prevention of computer crime, which is decisively influenced by the time factor (Stamenković et al., 2014, p. 6).

The CETS 185 regulates the specifically applicable methods of action of state bodies in investigations related to high-tech crime, as well as the minimum standards of protection against abuse of great powers that state bodies acquire in order to effectively combat high-tech crime.[10] That is why CETS 185, which adapts "classic" procedural measures to the conditions of the digital era, is of great importance for the practical work of special police units and prosecutor's offices for high-tech crime, especially if one keeps in mind that in the digital era, the crime scene is at a long distance from the place where the perpetrator is, often on the therritory of another country.

According to the provisions of the CETS 185, the contracting parties are obliged to adopt legislative and other measures in order to effectively conduct investigations and criminal proceedings, both in respect of criminal offenses that can be considered computer crimes and other crimes that can be committed through a computer system. These measures also concern the collection of evidence against perpetrators in electronic form, which is regulated in procedural part (II) of the CETS 185. Articles 16–21 define and prescribe procedural measures that enable urgent storage of computer data, storage and partial storage of traffic data, search and seizure of stored data, collection of data and traffic data in real time, as well as interception of data on the content of communication. From the point of view of the needs of practice, the provision of Article 19 of the CETS 185 (data order) which, according to Stamenković et al. (2017: 26), is a flexible measure that members of the detection authorities could apply in different cases, especially in those moments when other types of measures, such as search orders, seizures, interception of communications and the like, require the fulfillment of more significant and demanding legal and technical conditions.

The provisions of Articles 23–35 regulate international legal assistance. States Parties may, without the permission of the other Contracting Party, access stored computer data available to the public, regardless of where the data are geographically located, access or receive, through a computer system in their territory, stored computer data located in another Contracting State if they obtain legal and voluntary consent from persons who have the legal authority to disclose data to it through that computer system (Article 32). The provisions of the CETS 185 also provide for mutual assistance in real-time data collection. Contracting States should provide such assistance in order to collect data relating to certain communications in their territory in real time, which are transmitted via a computer system. This type of assistance shall be provided in accordance with the conditions and procedures provided for by national law, within the time frame and for similar offenses prescribed by national law. Mutual assistance for the purpose of collecting and providing relevant data shall be provided in accordance with the mutual legal assistance agreements of the signatory countries and their national legislation.

10 CETS 185 also provides initiatives for inclusion of material criminal law norms, some procedural aspects of criminal acts relicts in digital space and first response measures in securing and handling traces and digital evidence.

The provisions of the CETS 185 aim to speed up mutual assistance, but the formality of the procedure stipulates that it lasts between 6 to 24 months (T-CY Cloud Evidence Group, 2016: 9) and is incompatible with the instability and rapid mobility of electronic evidence. "Cloud computing" imposes the need to "circumvent" the limitations of the territorial jurisdiction of national authorities and establish the possibility of direct communication with providers, as indicated in the report of the T-CY Cloud Evidence Group (2016: 11), because data is increasingly distributed across multiple providers and locations, and is rarely found on a device or in a closed network.

## CHARACTERISTICS OF THE NATIONAL NORMATIVE FRAMEWORK

In the legislation of the Republic of Serbia, procedural measures related to electronic evidence are provided either by the Criminal Procedure Code – CPC (Official Gazette RS, 72/2011), or as part of special procedures of bodies responsible for conducting investigations into criminal offenses that can be committed by using information communication technology.

The CPC stipulates that evidence can be collected in several ways. Some of them are: using records as evidence, checking accounts and suspicious data (obtaining data, monitoring suspicious transactions, temporarily suspending suspicious transactions), seizure of items, secret surveillance of communication, video and audio recording, etc. There is no legal definition of electronic evidence, it is only provided that, for the purposes of proof, computer data suitable or intended to serve as evidence of a fact established in the procedure may be considered a document (Article 2, paragraph 1, line 26 in conjunction with Article 83, paragraphs 1 and 2). The precondition for further use is the same as for other evidence, and that is to be obtained in a lawful manner. In Article 2, paragraph 1, lines 29–32 of the CPC are defined: electronic record, electronic address and electronic signature, which would be relevant for determining the concept of electronic evidence. An electronic record is audio, video or graphic data that is in electronic (digital) form. An e-mail address is a series of characters, letters, numbers and a signal that is intended to determine the destination of the connection. The term electronic document, which is a set of data defined as electronic document, is interpreted in accordance with the definition from the law governing the electronic documents. An electronic signature is considered to be a set of data that is defined as an electronic signature, in accordance with the law governing electronic signatures.

According to Article 2, paragraph1, line 4 of the Law on Electronic Document, Electronic Identification and Trust Services in Electronic Business – ZED (Official Gazette RS, 94/17, 52/21) electronic document is a set of data composed of letters, numbers, symbols, graphics, audio and video materials, in electronic form. Having in mind the frequency of use of electronic documents, Article 7 of the ZED stipulates that such document cannot be challenged for validity, probative value, or written form simply because it is in electronic form. According to ZED, the original electronic document was originally created in electronic form (Article 10, paragraph 1), but a digital record identical to the original is also considered original (Article 10, paragraph 2). From the point of view of the possible use of an electronic document as evidence in criminal proceedings (or other court proceedings), the provisions of the ZED (Articles 11 and 12) governing the procedure and powers of public authorities regarding the certification of digitized or printed electronic documents (copies) are important. These provisions clearly favor the probative value of electronic records in official records kept on the basis of law, for which the presumption of reliability applies.

Defining the concept of the original document in electronic form is also important for the interpretation of the provision of Article 139 of the CPC, according to which the document is obtained by the agency or legal person in charge of procedural actions or the parties submit it, as a rule, in the original. Only if the original document has been destroyed, disappeared or cannot be obtained, a copy of the document can be obtained. As the same digital record is legally equated with a paper original, it should be possible to use a paper original, electronic document, electronic image or printed electronic document in court proceedings under equal conditions, which is not the case now. Avoiding unnecessary printing of electronic documents, for the needs of mutual communication between institutions, would provide speed and significant savings.

The CPC allows the use of electronic evidence, but does not determine the content of that term, which has already been pointed out in connection with the previous CPC in the research of Komlen Nikolić et al. (2010: 80). The content of special secret investigative actions allows the conclusion that they should be undertaken with the use of computers and modern devices in order to intercept data that are exchanged in cyberspace and obtain electronic evidence. As for the "open" procedural actions, Article 104, paragraph 2 provides for the possibility of online examination of particularly sensitive categories of witnesses, Article 147, paragraph 1 seizure of devices for automatic data processing and equipment on which electronic records are stored or can be stored, search of these devices (Article 152, paragraph 3) and procedure of their search (Article 157, paragraph 3). To date, the CPC has been amended several times (four times only until the entry into force), but the legislator did not consider that the specifics of the use of electronic data should be further regulated, although they are specific to the extent that they cannot be identified with material evidence.[11]

The seizure of electronic evidence is carried out in accordance with the CPC and the law ratifying the CETS 185. The handling of data from electronic communications by operators and competent state bodies for the purposes of conducting criminal proceedings or security protection are regulated by the Law on Electronic Communications (Official Gazette RS, 44/2010, 60/2013, 62/2013, 95/2918). Its provisions prescribe the manner of legal interception of electronic communications, the obligation to keep records by operators and competent state authorities on undertaking such activities, providing the necessary technical and organizational conditions to ensure the protection of such data, and which can be retained if necessary for record keeping, criminal proceedings or security protection of the Republic of Serbia. In addition, the Law prescribes both the form in which such data are retained, as well as the quality and level of their protection in order to preserve them for the aforementioned purposes (Articles 126–130a) Thus, on the basis of Article 147 of the CPC, seized and temporarily confiscated computers and mobile phones are sealed and opened in the presence of the accused and the witness, and after a forensic image is taken, they are sealed again in the presence of the same persons. According to the CPC, electronic evidence is treated as physical property (material evidence): when the evidence is collected, it is sent to the prosecutor, and forensic experts keep reports that are used later in the trial. The plaintiff keeps that evidence, i.e. deposits it until the indictment is submitted to the court. Although it is prescribed that the prosecution is responsible for the safe storage of evidence in adequate conditions, when it comes to electronic evidence, it is necessary to predict in detail what is meant by this, the question of the integrity of evidence is raised and their change is risky (it can be

11 Electronic data is not tangible, in electronic exchange only a copy of the original data is usually transferred (to the device on which it is stored or as a printout on paper). If they are on the internet, it is possible to access them (but also take them away) from anywhere in the world, they are transmitted with great speed, regardless of national borders, it is easier to create, process and hide their traces anonymously. There is a great risk of altering the original data during further manipulation of the obtained evidence, because it must be converted into a readable format that allows its further processing implies the risk of intentional, unintentional, and even unnoticed manipulation of the original information.

unintentional or even unrecognized).[12] Moreover, in criminal matters, it is necessary to ensure the reliable permanent storage of some electronic records that have great potential for later use as evidence (for example, data from prosecutorial files on unfinished investigations or from police files relating to unsolved criminal cases).

In the research of Komlen Nikolić (2010), it was emphasized that the urgent protection of electronic data from the CETS 185 is not ensured by the rules of the CPC. As the authors stated in the previous part of this paper, such protection is defined by the Law on Electronic Communications. However, the prosecutor's obligation to address the court in order to obtain an order for the implementation of a certain measure certainly calls into question the urgency of action.

Adequate enforcement of the law requires continuous training of judges and prosecutors in obtaining, processing and using electronic evidence along with advances in technology, because prosecutors need to take care of their collection and security, and judges need to decide on factual issues based on disputed electronic evidence, and not experts who record that evidence or digital forensic scientists who will discover and expertise it. An expert may be engaged in gathering evidence, but there should be no obligation for him or her to be present when the prosecutor presents evidence from the indictment at the main trial. Experts may be hired only if required by the court, the prosecution or the defense, which is an additional cost for the prosecution or the court (CoE Assessment report, 2018). A particular problem may be the contestation of evidence by the expert adviser of the opposing party during the proceedings. When it comes to criminal acts that fall under the jurisdiction of special departments of the court and public prosecutor's office for organized crime and special departments for the fight against corruption, it is possible to use the knowledge and skills of financial forensic scientists when collecting electronic evidence. However, the question is to what extent they possess the knowledge and skills necessary to recognize electronic evidence and use it in criminal proceedings.[13] Therefore, it is necessary to organize specialized trainings for them as well.

Based on the CETS No. 185, different jurisdictions can exchange data through contact points or requests for mutual legal assistance, and this option is used by the competent authorities of the Republic of Serbia. However, shortcomings are also noted here that jeopardize the efficiency of investigations, both in yhe CETS 185 itself and in the application of domestic legislation.

The establishment of international cooperation through mechanisms of mutual justice assistance may take too long, thus increasing the risk that data may be deleted or altered. Electronic evidence should be seized on a portable device, because the seizure of hardware or related devices is outdated, and may impede the economic activity of legal entities that did not participate in the criminal act of their employee. The problem of obtaining evidence of illegally acquired property of the suspect in cryptocurrency is also pronounced, because the data can be easily deleted, which indicates the need to find and record data on the existence of such property when searching and collecting electronic evidence (CoE Assessment report, 2018).

Since 2011, the criminal procedure in Serbia has been modified according to the adversarial model, in which the testimonies of witnesses and defendants, obtained directly at the main trial, in oral and adversarial hearings, have a special evidentiary significance.[14] During the state of emergency in Serbia (from March 15 until May 6, 2020) due to the epidemic of the SARS-CoV-2 virus, when criminal courts acted only in emergencies, the problem of applying online hearings came to the fore. The issue

14 Therefore, Anglo-Saxon law specifically regulates the admissibility of electronically recorded statements, see: Model Law of Electronic Evidence, 2017; The Uniform Electronic Evidence Act in Canada, 2011, according to Duranti, Rogers & Sheppard, 2020.

of protection of the rights of the defendants and the probative value of the testimony given in the online hearing thus undertaken were also in questions.

The so-called trials via Skype were organized on the basis of written information from the Ministry of Justice to be applied in urgent proceedings against persons who do not respect self-isolation decisions, who are usually sentenced to three years in prison. Subsequently, the Government adopted a Decree on the manner of participation of the accused in the main trial in criminal proceedings held during the state of emergency declared on March 15, 2020 (Official Gazette RS 49/20). The Decree allows the accused to testify online if the judge declares that the presence of the accused at the main trial is not safe due to the danger of spreading the infection, and there are technical condition for the accused to be heard online. Because the Decree derogates from the CPC, which does not provide for such a possibility, and because the right to a fair trial has been violated, lawyers and NGOs have sent an initiative to the Constitutional Court to review the Decree, which the Court has not yet ruled on. This example, as well as previous observations, show that our normative framework needs to be supplemented by amendments to the CPC or the adoption of another legal act whose application would be allowed in criminal proceedings, to regulate the specifics of using electronic evidence, perhaps in general for all proceedings (judicial and administrative) as shown by the examples of the above acts of the Commonwealth and Canada. In addition, a way of facilitating international cooperation must be envisaged, as indicated by the reasons for the latest legislative initiatives in the EU regarding electronic evidence.

## EUROPEAN INITIATIVES AND DIGITALIZATION OF JUSTICE

Since 2016, regulations have been prepared in the EU that would facilitate the acquisition, exchange and use of e-evidence, in various ways. They have been designed at least twice: E-Codex Initiative and Project EVIDENCE Road. The former should provide the necessary infrastructure for a reliable and secure exchange of requests and evidence, while the latter should provide a methodology and formal language to enable a reliable and secure exchange (Biasiotti, 2017: 2). In mid-2019, the European Commission undertook activities to conclude a cooperation agreement with the United States, to enable the use of "Cloud" evidence and to prepare the Second Additional Protocol to the CETS 185. The pragmatic reason was that research showed that 2/3 of e- evidence were localized in another EU country or in a third country outside the EU (Tinoco-Pastrana, 2020: 46–47). Efforts are being made to facilitate access to electronic evidence circulating or stored outside the EU, and these agreements should simplify legal aid mechanisms and increase its efficiency through direct cooperation with service providers and shortening deadlines for access to electronic data. To the same end, cross-border cooperation has been facilitated within the EU.

The digital environment imposes the need that cross-border cooperation in all crimes committed through computer systems or the internet, when there may be a conflict of jurisdiction of different jurisdictions, must be developed through different mechanisms in relation to the procedure of mutual international assistance. Therefore, in October 2020, the Committee of the European Parliament for Civil Liberties, Justice and Home Affairs adopted the report on the legal proposals from 2018 on electronic evidence in criminal proceedings.[15] The new rules should allow Public Prosecutor's Office to directly request to obtain electronic data necessary to investigate and prosecute perpetrators from electronic service providers operating in the EU, regardless of where the data is stored. Accordingly, service providers should appoint an authorized person (representative) to provide evidence and respond to requests submitted to applicants (competent authorities) (Bakowski & Vornova, 2020).

The Communication of the European Commission COM (2020) 710 final of December 2020 emphasizes the need to harmonize the regulations of the member states regarding access to digital information and evidence. This would facilitate access to evidence located in the territory of another jurisdiction (whether it is an EU member or a third country) (EC COM (2020) 710 final).

In the mentioned document, the EC states that in order to improve the national judicial systems for the sake of digitalization, it is necessary to improve the transnational cooperation of the competent authorities. Such cooperation implies full respect for the human rights guaranteed by the EU Charter of Fundamental Rights. Different challenges due to the existence of differences still exist at the level of member states, such as, for example, the possibility of access to electronic evidence in cases before the competent courts. According to the EC, in the coming period it should be possible for evidence to be submitted to the court exclusively in digital format. This should allow the exchange of a large amount of data in different formats. Therefore, the EU should provide financial support to member states, support in amending regulations in order to meet the requirements regarding digitalization, which would enable better access to justice and promote transnational cooperation, including the field of artificial intelligence. Legal representatives need to be trained to provide support to their parties in order to communicate with the judiciary and submit documents in a safe and efficient manner. In addition to transnational cooperation, member states should enable cooperation between relevant national institutions and the secure and efficient exchange of information with judicial and prosecuting authorities. Electronic signatures and stamps should be accepted when submitting evidence in the same way in all member states. Regulations at the national level should enable the processing of personal data in accordance with the provisions of the General Regulation on Personal Data Protection, and therefore the report of the competent ombudsman has been requested (EC COM (2020) 710 final: 2–5, 10).

The Office of the European Public Prosecutor, Europol and Eurojust should have an adequate level of cooperation with both member states and non-member countries, but it is necessary to provide assistance and support to Europol and Eujust. The efficiency of such cooperation would be enhanced by cooperation in electronic environments. This would facilitate and expedite communication by enabling the joint work of joint investigation teams in conducting transnational investigations (EC COM (2020) 710 final: 17). Such cooperation would reduce administrative costs and facilitate access to various registers relevant to gathering evidence.

## CONCLUSION

Criminal law must keep pace with technological changes by regulating the possibility for electronic data to be used as evidence in criminal proceedings. In Serbia, as well as throughout Europe, there is a lack of special regulations in this area (both quantitatively and qualitatively). Walken (2018: 227) also states that the normative frameworks, in the countries where they exist, are fragmentary and do not explicitly refer to criminal proceedings, while, on the other hand, legal gaps are filled by interpreting the provisions relating to material evidence. The practice, however, requires explicit rules to be made, for example, on obtaining electronic data from any third party other than the telecommunications service provider, on obtaining information between devices, on preliminary data retention measures ("expedited preservation of stored computer data"), on handling large amounts of Big Data and procedures that guarantee and confirm the integrity and authenticity of the data set (Walken, 2018: 227).

Procedural legislation of the Republic of Serbia should be supplemented to ensure full implementation of the CETS 185. It lacks special rules that will more fully regulate the use of electronic evidence

in modern conditions, in order to strengthen legal equality of citizens and establish more efficient cooperation of competent authorities at the national level and international prosecution and the trial of perpetrators. Possible obstacles are the need for an interdisciplinary approach when adopting such rules, the need to standardize the exchange of electronic data on one or fewer platforms (following the example of the E-government web portal or similar), continuous education of public sector employees to recognize evidence in electronic form and ensure its integrity. Submiting data in digital form through electronic communication systems would simplify the procedure, enable a trial within a reasonable time and would be a saving for those institutions that are authorized applicants for criminal charges. Direct submission of data to the competent judicial authorities would save time and prevent the integrity of the evidence from being compromised, especially if the storage is used adequately.

In the digital age, mutual legal assistance established through diplomacy is an inefficient solution. According to the latest proposals of EU legislation, the limitations of competences arising from territorial sovereignty should be overcome by allowing the competent authorities to directly request the necessary electronic data for prosecution and proceedings from service providers who would have special legal representatives in charge of those services. The EU regulations on electronic evidence, which are expected to be adopted soon, mark a new stage in the development of judicial cooperation, within the EU and beyond, because they represent a segment in the general effort to prevent dangerous forms of crime committed in that area or by using computers. It will be increasingly difficult to fit into these requrements, if our regulations are not improved in time.

## REFERENCES

1. Bakowski, P. &Vornova, S. (2020). Electronic Evidence in Criminal Matters. European Parlamentary Research Service. https://www.europarl.europa.eu/thinktank/nl/document.html?reference=EPRS_BRI%282021%29690522. Accessed on August 20, 2021.
2. Biasiotti, M-A. (2017). A proposed electronic evidence exchange across the European Union. *Digital Evidence and Electronic Signature Law Review* 14(1): 1 –12. https://journals.sas.ac.uk/deeslr/article/view/2337/2289- Accessed on August 20, 2021.
3. CETS 185 – Explanatory Report to the Convention on Cybercrime (200.1). https://rm.coe.int/16800cce5b. Accessed on August 20, 2021.
4. CoE Assessment report (2018). Assesment report on the acquisition and use of electronic evidence in criminal proceedings under domestic law in the countries of Southeast Europe and Turkey, version of March 5, 2018. https://rm.coe.int/3156-52-iproceeds-electronic-evidence-report-serbian/16807bdfe3. Accessed on August 20, 2021. EC COM (2020) 710 final.
5. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Region, Digitalisation of justice in the European Union. A toolbox of opportunities, Brussels, December 2, 2020. https://ec.europa.eu/info/sites/default/files/communication_digitalisation_en.pdf. Accessed on August 20, 2021.
6. Council of Europe, Convention on Cybercrime (CETS No 185), Budapest, November 23, 2001. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561. Accessed on August 20, 2021.

7. Council of Europe, Cybercrime Division (2020), Summary report, Meeting of the 247 points of contact (CP) of the Budapest Convention on Cybercrime, November 2020. https://www.coe.int/en/web/cybercrime/all-reports. Accessed on August 20, 2021.
8. Charter of Fundamental Rights of the European Union (2016). *OJ* C 202, 7. 6. 2016, pp. 403–403. ELI: http://data.europa.eu/eli/treaty/char_2016/art_47/oj. Accessed on August 20, 2021.
9. Criminal Procedure Code – CPC, *Official Gazette of the Republic of Serbia*, Nos. 72/2011, 101/2011, 121/2012, 32/2013, 45/2013, 55/2014, 35/2019, 27/2021 – US decision and 62/2021 – US decision.
10. 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, Strasbourg, April 17, 2018, COM(2018) 226 final, 2018/0107(COD), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A226%3AFIN, Accessed on August 20, 2021.
11. Duranti, L., Rogers C. & Sheppard, A. (2020). Electronic Records and the Law of Evidence in Canada: The Uniform Electronic Evidence Act Twelve Years Later. *Archivaria,* 70, 95–124, https://archivaria.ca/index.php/archivaria/article/view/13296. Accessed on August 20, 2021.
12. EC COM (2018) 225. Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters. April 17, 2018. 2018/0108 (COD).
13. EC COM (2018) 226. Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings. April 17, 2018. 2018/0107(COD).
14. EC COM (2020) 710 final. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the Region, Digitalisation of justice in the European Union A toolbox of opportunities, Brussels, December 2, 2020. https://ec.europa.eu/info/sites/default/files/communication_digitalisation_en.pdf. Accessed on August 20, 2021.
15. EC ECEPRS: BRI (2021) 690522_EN. Briefing EU Legislation in Progress, https://www.europarl.europa.eu/etudes/BRIE. Accessed on August 20, 2021.
16. EC COM (2020) 710 final. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Digitalisation of justice in the European Union, a toolbox of opportunities Brussels, December 2, 2020, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2020:710:FIN. Accessed on August 20, 2021.
17. Enhanced Cooperation and Disclosure of Electronic Evidence: Towards a New Protocol to the Budapest Convention on Cybercrime, https://www.coe.int/en/web/cybercrime/enhanced-cooperation-and-disclosure-of-electronic-evidence-towards-a-new-protocol-to-the-budapest-convention. Accessed on August 20, 2021.
18. Europol (2018). Internet Organised Crime throat Assessment (IOCTA), https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018. Accessed on August 20, 2021.
19. Europol (2020). Internet Organised Crime throat Assessment (IOCTA), https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020. Accessed on August 20, 2021.
20. General Data Protection Regulation (2016). 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, May 4, 2016, pp. 1–88. ELI: http://data.europa.eu/eli/reg/2016/679/oj. Accessed on August 20, 2021.

21. Komlen Nikolić, L., Gvozdenović, R., Radulović, S., Milosavljević, A., Jerković, R., Živković, V., Živanović, S., Reljanović, M. & Aleksić, I. (2010). *Suzbijanje visokotehnološkog kriminala*. Beograd: Association of Public Prosecutors and Deputy Public Prosecutors.
22. Law on Ratification of the Convention on High-Tech Crime, *Official Gazette of the Republic of Serbia*, No. 19/2009.
23. Law on Ratification of the United Nations Convention against Transnational Organized Crime and Additional Protocols, *Official Gazette of the Federal Republic of Yugoslavia – International Agreements*, No. 6/2001.
24. Law on Electronic Communication, *Official Gazette of the Republic of Serbia,* Nos. 44/2010, 60/2013 – decision of the Constitutional Court, 62/2014 and 95/2018 – other law.
25. Law on Electronic Document, Electronic Identification and Trust Services in Electronic Business – ZED, *Official Gazette of the Republic of Serbia*, Nos. 94/17, 52/2021.
26. Law on Organization and Competence of State Bodies in the Suppression of Organized Crime, Terrorism and Corruption, *Official Gazette of Republic of Serbia,* Nos. 94/2016, 87/2018 – other law.
27. Model Law of Electronice Evidence 2017. Office of Civil and Criminal Justice Reform.: The Commonwealth. https://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_7_ROL_Model_Bill_Electronic_Evidence_0.pdf. Accessed on August 20, 2021.
28. Press release, January 12, 2021. Darkmarket: world's largest illegal dark web marketplace taken down, press release, January 12, 2021. https://www.europol.europa.eu/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down. Accessed on January 20, 2020.
29. Stamenković, B., Balota, A., Pavličić, V., Paunović, B. & Backović, J. (2014). *Visokotehnološki kriminal,* A practical guide to contemporary criminal law and case studies. Podgorica: OSCE Mission to Montenegro.
30. Stamenković, B., Živanović, S., Paunović, B. & Stevanović, I. (2017) Vodič za sudije i tužioce na temu visokotehnološkog kriminala i zaštite maloletnih lica u Srbiji. Belgrade, Save the Children. A practical guide to modern criminal law and practical examples. Podgorica: OSCE Mission to Montenegro.
31. Tinoco-Pastrana, Á (2020). The Proposal on Electronic Evidence in the European Union. *EuCLR European Criminal Law Review* 1, 46–50, https://doi.org/10.30709/eucrim-2020-004 /. Accessed on August 20, 2021.
32. Tropina, T. (2012). The Evolving Structure of Online Criminality. How Cybercrime is Getting Organised. *EUCRIM* 4/2012, 158–165, https://www.corteidh.or.cr/tablas/r15111.pdf. Accessed on August 20, 2021.
33. T-CY Cloud Evidence Group, Criminal justice access to data in the cloud: cooperation with "foreign" service providers, May 3, 2016. https://www.coe.int/en/web/cybercrime/ceg. Accessed on August 20, 2021.