Matijašević Jelena[*]
https://orcid.org/0000-0001-8068-0816
Bingulac Nenad[**]
https://orcid.org/0000-0003-1187-7054
Marinković Darko[***]
https://orcid.org/0000-0002-7833-7653

UDC: 343.1:004
Original scientific paper
DOI: 10.5937/ptp2404018M
Received on: November 10, 2024
Approved for publication on:
December 9, 2024
Pages: 18–33

DIGITAL EVIDENCE IN CRIMINAL PROCEEDINGS – CHALLENGES AND SOLUTIONS

ABSTRACT: In the last decade, digital evidence in criminal proceedings has become a key tool in modern forensic investigation, with the help of which it is possible to identify, analyze and verify information that can be crucial for making a decision in court proceedings. Digital data, through the perception of various forms of electronic records, are increasingly becoming the basic evidence in criminal cases, and because of this, no distinction is made between existing material evidence and modern digital evidence. In this research, the importance of digital evidence, its advantages and challenges in collection and processing, as well as the legal and ethical aspects of its use in criminal proceedings were pointed out and indicated. The importance of the methodological approach in the forensic analysis of digital evidence was also pointed out, all in order to achieve the admissibility of digital evidence before a criminal court. The challenges and opportunities presented by this evidence are drawn throughout the research and pointed out. The hypothesis of this research is contained in its title and refers precisely to controversial issues and the legislative application of digital evidence in criminal proceedings. The aim of the

[*]LLD, Full Professor, Vice Dean for Science, University Business Academy in Novi Sad, Faculty of Law for Commerce and Judiciary in Novi Sad, Novi Sad, Serbia, e-mail: jelena@pravni-fakultet.info
[**]LLD, Associate Professor, University Business Academy in Novi Sad, Faculty of Law for Commerce and Judiciary in Novi Sad, Novi Sad, Serbia, e-mail:nbingulac@pravni-fakultet.info
[***]LLD, Full professor, University of Criminal Investigation and Police Studies, Belgrade, Serbia, e-mail: darko.marinkovic@kpu.edu.rs

work is to consider this topic by looking at the new regulation and directive that have been passed and will only be adopted in 2026, but in principle to consider the issue of digital evidence through practice because this topic remains crucial for the further development of the judicial system in the digital age. During the writing of this research, an analytical method was used in order to consider the legislation of the European Union, and make a comparison with the domestic legislation. Then, the normative method was used when considering the criminal procedure and defining digital evidence, and certainly the deductive method was also used.

Keywords: *digital evidence, criminal law, criminal procedure, European legislation, forensic analysis.*

1. Introductory considerations

When the term digital evidence is mentioned, the first thing that often comes to mind is high-tech crime and ways of knowing, discovering and of course proving certain criminal acts that were committed with the help of computers, computer networks, the Internet, etc. (Matijašević, 2012, p. 399). It was mentioned correctly, but it was inadequately framed and predefined only for a certain form of criminality.

Realistically, they have been one of the most important sources of information for years, and it is impossible to imagine a modern criminal procedure without such evidence, as crimes do not necessarily have to be complex or qualified as more serious by the criminal code (Criminal code, 2005).

Structurally, digital evidence can include a wide range of information depending on the type of digital record. Given that the goal of this work is to consider digital evidence in the prism of criminal legislation, the code and algorithm of digital records will not be considered, but will be referred to in the broadest sense with the aim of bringing them closer together, ie reducing their abstractness as evidence to a logical minimum. In this context, digital data that can be valorized as evidence are: digital data from computers, mobile phones, cloud systems, internet searches, e-mails, messages on social networks, then as digital data that are increasingly represented in the evidentiary process are and footage from security cameras, other digital devices, but certainly also geolocation data.

It is completely understandable that the creation of new judicial practice and the inclusion of new forms of evidence in the procedural system require at

least elementary education of the court, the prosecution and defense attorneys, regardless of the fact of the key role of specialist experts. Every innovation in the procedure that unquestionably aims to fulfill the norms of criminal and criminal procedural law brings with it significant challenges in terms of legal validity, methodology of data collection and processing, as well as protection of the rights of the accused. The development of digital technologies and their increasing presence in everyday life can soon easily become basic evidence, but also transform the way in which crimes are investigated and determined.

What has been pointed out so far about digital evidence has the impression that it is about something that is still in its infancy, that is, something that still needs to be thought about. In reality, the circumstances are different.

The ubiquity of computers and their presence led to the creation of the first digital evidence in the second half of the 20th century. The first cases where digital data was used as evidence date back to the 1980s (Reith, Carr & Gunsch, 2003, p. 3). Although Canada was the first country to adopt digital evidence into its legal legislation in 1983 through amendments to the Criminal Code (Casey, 2004, p. 26), it is considered that the first concrete application of digital forensics followed as early as 1984 in the United States of America through the institutionalization of digital evidence, which led to enabling the legal use of data with computer systems (Tompkins & Mar, 1986, p. 461). Those pioneering digital evidences were not widely accepted by the courts and the prosecution because of the high degree of ignorance of their interpretation, since they were still sophisticated technical data.

With the progress of the Internet and the development of software solutions and of course computers in general in the early 2000s, digital evidence became crucial in solving cases involving fraud, identity theft, and slowly became important for solving more serious forms of crime such as pedophilia and terrorism (The Evolution of Digital Forensics, 2024). When it comes to Europe, certainly the most significant shift in the issue of digital evidence followed in 1999, when the European Union adopted the Directive on the protection of evidence in digital form (Macan, 2021, p. 188).

Being aware that today almost everything is directly or indirectly connected to computers, computer systems, smartphones, smart devices, etc. and that in terms of software, the incredible increase in the number of applications used has drastically increased the amount and type of potential digital evidence that could be used in the criminal process. In addition to classic sources such as data from hard drives, data from mobile devices, GPS location, social media records, digital video and audio materials, and even data collected via the Internet (IoT) can be used today. In the mentioned sense,

the role of digital evidence in criminal proceedings can become in certain cases and exclusively crucial not only because of the amount of data that can be available, but also because of their power to accurately show the dynamics of events and the behavior of suspects or victims.

To clarify, digital evidence does not only play a significant role in solving criminal offenses in proceedings before domestic courts. Being aware that computer networks, applications, etc. with international databases, therefore, digital evidence is of particular importance in the investigation of international crimes, because based on its specificity, there is a rapid exchange of information between states and interstate coordination (Ragni, 2023, p. 2). In this sense, one of the most significant international frameworks is the Budapest Convention on Cybercrime from 2001 and various standards where standards for the use of digital evidence are established (The Convention on Cybercrime, 2021). In a practical sense, the signatory states gradually began to form specialized units for digital forensics, which also resulted in the education of experts who will deal with the analysis of digital data.

2. Digital evidence in criminal proceedings from the perspective of EU legislation

We will begin this part of the research with a brief review of the so-called The Budapest Convention with an indication of the question of what are its advantages and impacts in the context of cybercrime.

Structurally, the Budapest Convention is not just a legal document. In fact, this is a framework that allows experts from practice from various countries and from the broadest aspect to exchange experiences and create relationships that facilitate cooperation in specific cases, including emergency situations as well as situations that are not provided for by the provisions of this Convention. One of the ideas of its existence is that each country can use the Budapest Convention as a guideline for creating its own legislation, but it can complete it and implement it in its legislation as a law. Moreover, membership in this agreement implies additional advantages (Council of Europe, 2001). Serbia is one of the signatory countries of this Convention.

When considering the benefits of the Budapest Convention, it is considered the most comprehensive and coherent international agreement on cybercrime and electronic evidence that exists today. In addition to the fact that it can be used as a guideline for domestic legislation, it has a significant role as a framework for international cooperation between the signatory states. The Budapest Convention provides for (I) the criminalization of conduct – from

illegal access, data and system interference to computer fraud and child pornography; (II) procedural powers to investigate cybercrime and secure electronic evidence related to any crime, and (III) for effective international cooperation operations (The Convention on Cybercrime, 2024).

Although non-signatory states can also use the Budapest Convention as a modality or source of domestic legislation, signatory states have additional benefits such as: (I) The Convention provides a legal framework for international cooperation not only in terms of cyber-crime – in terms of illegal acts against and with the help of computers, but also in relation to any criminal offense that can be proven with electronic evidence. (II) Signatories to the Convention may sign and ratify the Second Additional Protocol to the Budapest Convention, which provides additional and accelerated tools for improved cooperation and which gives additional importance to electronic evidence. In addition to the aforementioned, direct cross-border cooperation as well as cooperation in emergency situations is also special. (III) Signatories are members of the Cybercrime Committee (T-CI) and share information and experience, assess the implementation of the Convention or interpret the Convention through the Guidelines Notes. (IV)- The Convention provides that if a new signatory state was not an initial signatory from 2001, it has the possibility to participate in the negotiations on future instruments and the further evolution of the Convention. (V) The signatory states cooperate with each other in reliable and efficient cooperation. There are indicators on the basis of which it is predicted that private sector entities will cooperate with the criminal justice authorities of the signatory states precisely because of interstate compliance and the existence of a legal framework that regulates the issue of cybercrime and digital evidence at the scene. (VI) And finally, states that are seeking to accede or that have recently acceded become priority countries for assistance in creating domestic legislation to address the issue of cybercrime and digital evidence. The indirect importance of the aforementioned is the improvement of international cooperation. One of the evaluations of this Convention shows that based on the experience of more than 20 years of its existence, there are no negative reasons for signing the Budapest Convention (Cybercrime, 2024).

When it comes to digital evidence regulated in the Budapest Convention, it is also important to mention that there is a Convention Committee on Cybercrime (T-CI) and C-PROC specialized cybercrime Program Office for Global Capacity Building that are available in the determination of digital evidence , which includes, in addition to the members of the Council of Europe, Canada, Japan, South Africa and the USA (Cybercrime Convention Committee, 2020).

Regulation 2023/1543 and directive 2023/1544 are particularly important for digital evidence in criminal proceedings from the point of view of European Union legislation. The regulation begins to apply from August 18, 2026, and the directive will have to be implemented into domestic legislation by February 18, 2026.

The main objective of Regulation 2023/1543 (Regulation 2023/1543) is to enable national judicial authorities involved in criminal proceedings to order service providers offering services in the European Union to produce or preserve electronic evidence wherever the data is located. Then, to facilitate and speed up cross-border access to electronic evidence as well as to prevent their deletion, while ensuring legal protection for the persons whose data is requested.

The key elements of Regulation 2023/1543 are that it applies to service providers providing one or more of the following categories of services in the EU: electronic communications; Internet domain names and IP numbering; communication, storage and processing services. The Regulation does not apply to providers providing: financial services (eg banking, lending, insurance, reinsurance, professional or personal pensions, securities, investment funds, payment and investment advice); services exclusively within their own EU member state.

A European Production Order, which is a Court Order ordering the handover of electronic evidence, and a European Preservation Order, which is a Court Order ordering the storage of electronic evidence, and which can be subsequently requested, can only be issued: during criminal proceedings and to enforce a sentence imprisonment or detention for at least 4 months; for specific data that service providers have. The authority issuing the European production order must notify the person whose data is requested. As a rule, this must happen without undue delay. The aforementioned may be postponed if, for example, it would jeopardize the investigation. A person can challenge the legality of the order before a court in the Member State that issued it (right to legal remedies).

According to this directive, a judge, court, investigating judge or public prosecutor can issue a European production or preservation order. Orders can be sent directly to a service provider in another Member State without the prior involvement of the authorities of that country.

European production orders must be: necessary and proportionate to the criminal proceedings; they must respect the rights of the suspect or the accused; it can be issued only under the same conditions as for a similar domestic case; must respect the immunities or privileges granted, as well as the determination and limitation of criminal liability in relation to freedom

of the press or freedom of expression, depending on whether they seek subscriber, identification, traffic or content data; include specific information, such as the issuing authority, the addressee, the requested data and time frame, the applicable criminal law provisions of the issuing Member State and a summary of the case. The European manufacturing order is sent to the service provider that controls the personal data (controller).

The European Preservation Order must be necessary and proportionate to prevent the removal, erasure or alteration of data that may subsequently be requested. It can then be issued for all criminal offenses if they could have been issued under the same conditions for a similar domestic case, include specific information, such as the issuing authority, the addressee, the requested data and time frame and the applicable provisions of the criminal law of the issuing Member State.

Requests are made via the European Production Order Certificate (EPOC) or the European Preservation Order Certificate (EPOC-PR), to a designated institution or legal representative of the service provider.

Addressees have the obligation, when it comes to the European Production Order, to act expeditiously, upon receipt of the EPOC, in order to preserve the requested data. Then they must deliver the data within 10 days, while in urgent circumstances they have the obligation to transfer the data within 8 hours. Addressees must notify both the issuing and enforcement authorities if they believe that the EPOC may infringe the right to immunities or privileges or the rules on the determination or limitation of criminal liability in connection with freedom of the press or freedom of expression. In the circumstances that the addressees cannot provide the data, they have the obligation to explain it to the issuing authority, without undue delay. Circumstances that may exist that affect the inability to provide the requested data are as follows: (I) The EPOC is incomplete, contains obvious errors, or does not provide enough information. In those circumstances, there is a period of 5 days to resolve the aforementioned. (II) If the data is unavailable due to circumstances beyond their control. (III) If there is any other reason for not complying with them, such as an order that could conflict with the law of the non-EU country where the data may be stored.

Addressees have the obligation, when it comes to the European Preservation Order, to act immediately, upon receipt of the EPOC-PR, to preserve the requested data. Then to store the data for 60 days, which the issuing authority may extend for an additional 30 days, after which storage ends, unless the issuing authority has in the meantime issued a subsequent request, for example through mutual legal assistance, for the data to be handed over or stored for the next 30 days. Finally, the addressees can object to the order on

the same grounds as for the EPOC – immunities or privileges, incomplete or obvious errors, circumstances beyond their control, other reasons.

At the end of pointing out the significant elements of Regulation 2023/1543, it is also necessary to point out that all written communication between national authorities and certain institutions or legal representatives of service providers takes place through a secure and reliable decentralized IT system (Juszczak & Sason, 2023, p. 183).

The main objective of Directive 2023/1544 (Directive EU 2023/1544) is to require that certain service providers offering services in the EU have certain institutions or appointed legal representatives in the EU in order to be able to receive and fulfill the orders of national authorities for the purpose of collecting electronic evidence in criminal proceedings.

This Directive directly applies to service providers that enable: electronic communications; Internet domain names and IP numbering; communication, storage and processing services. It is important to note that the Directive does not apply to suppliers who supply: financial services e.g. banking, lending, insurance, reinsurance, occupational or personal pensions, securities, investment funds, payment and investment advice; nor to suppliers who provide their services exclusively in their own country.

Member States, in addition to the implementation of this Directive, have the obligation to establish rules on penalties for non-compliance and to designate one or more central authorities to ensure the proper implementation of the Directive.

The Digital Evidence Directive is the result of compromises and negotiations between the European Parliament, the Council and the Commission, all with the aim of appropriately balancing the interests of smooth enforcement of the law on the one hand and adequate protection of fundamental rights and preventing abuse in favor of the individual. New legislative instruments enable judicial and prosecutorial authorities to have the possibility to initiate a case based on digital evidence, for which there were certain obstacles in international relations.

In this regard, refusal to execute orders from foreign courts have been eliminated and, in essence, exist only in the case of traffic and content data. Given the limitations and short deadlines, it may be questioned whether the Orders can be effectively reviewed. Practice will show whether the new rules for collecting electronic evidence represent progress (Wahl, 2023, p. 166).

It should also be noted that the Digital Evidence Regulation and Directive are only one of the segments in terms of acts dealing with online law enforcement. In addition to the aforementioned, there is also the EU

Digital Services Act (DSA), which introduced responsibilities and a system of accountability and transparency for intermediary service providers, and Regulation 2021/784, which regulates the duties of care to be applied by hosting service providers to remove or disable access to terrorist content on network (Wahl, 2023, p. 168).

It remains to be seen whether the new EU rules on digital evidence are adequate and sustainable as a model in other countries or in multilateral conventions at the international level (Propp, 2024).

3. Admissibility of digital evidence in domestic law

We leave digital data, i.e., "digital signatures" all around us, and that is no longer in question. Is it some form of targeted marketing (Sulcas, 2024) or is it about leaving personal traces when using the Internet (Oxford, 2024) or is it about online shopping where particularly sensitive data is left (Camp, 2024), biometric data with which we store smartphones, security cameras, etc. We leave a certain amount of digital data all around us.

All these digital data can at some point become digital evidence as important sources of information that can be used in court proceedings. One can clearly see the position that "every digital record in criminal proceedings should have the status of a document, which supports the indictment in the same way as other material evidence" (Bajović, 2024).

The Code of Criminal Procedure stipulates that the term "document" is considered, based on Article 2 paragraph 1 item 26, any item or computer data that is eligible or determined to serve as evidence of a fact that is established in the procedure (Criminal Procedure Code, 2011).

Certain scientific studies were conducted in which the issue of relationships was discussed, for example. recordings from security cameras in public places and the right to privacy that may be called into question due to inappropriate and unauthorized manipulation of that data (Kovačević, 2013, p. 1796). In such circumstances, there must be a balance between the right to privacy and the need to detect criminality (Bajović, 2024), especially if there are circumstances in which public security cameras record a serious crime, e.g. murder, and the perpetrator can be identified based on the video (Miljuš, 2024).

It has been mentioned on several occasions how widespread digital data is through the use of mobile phones, computers, etc. but precisely because of that prevalence and their great use, all these data can be, as already said, a significant evidentiary resource, while on the other hand, precisely because of their form, digital, and the way they are stored, they can be quite sensitive in

terms of permanence, in other words, they can are easily damaged. Then they can be manipulated afterwards, which may or may not be easily noticeable, which would certainly absolutely degrade it as an evidentiary element (Mihajlović, 2024).

Precisely because of all the above, it is necessary to have people who know how to recognize subsequent manipulations with digital evidence, but also people who know how to take them and use them in criminal proceedings in an adequate way. In addition to trained experts, it should be taken into consideration that such persons exist in the prosecutor's office and the court. Computers, telephones and similar devices are confiscated with the presence of witnesses and the creation of a forensic photograph, after which they are transferred to the prosecutor's office, while only the reports remain with the forensics.

The collection of digital evidence is carried out in an identical way as when conducting a judicial search of property and persons, which in practice can raise certain procedural issues and create problems.

Guidelines on the seizure of electronic evidence are set out in the Law on Criminal Procedure and the Law on the Ratification of the Convention on High-Tech Crime, but there are no specific domestic guidelines on the subject. On the other hand, there are police instructions or guidelines for the seizure of electronic evidence (Iproceeds, 2024).

The same report states the following: "Serbia has experience with the use of electronic evidence in court." Courts accept that evidence is presented in digital form, while expert reports are submitted in printed form. Courts have equipment for dealing with electronic evidence and for reviewing electronic evidence. They also have experience in handling cases where forensic analysis of electronic evidence has been used" (Iproceeds, 2024).

The process of displaying digital evidence in criminal court proceedings is not a simple action, but given that the data is presented by an expert, a very long impression is made. The mentioned expert must have extensive experience in the field of information technologies, then he must have knowledge of operating systems and, of course, forensic analysis. Sometimes, only one expert is not enough to master specially encrypted digital data. One of the peculiarities when it comes to digital evidence is that from the moment of discovery to the conclusion of the forensic analysis, that evidence should always be treated as when it will be presented, that is, it must be objective, accurate, convincing and understandable (Petrović, 2024, p. 8).

In practice, parties in criminal proceedings have their own experts who are entrusted with the analysis and forensics of digital evidence, which often leads to cross-examination and confrontation of the opinions of two experts who have,

or at least should have, the same knowledge and experience. Certain studies indicate that cross-examination of experts is a deterrent factor, because experts, as stated in one study, "refuse court expertise and confrontation of opinions with another equally good court expert and prefer to accept the role of a neutral expert consultant to the prosecutor or the judge himself" (Petrović, 2024, p. 8). Given that it is often binary data that is stored or transmitted in digital form, and which has a certain evidential value in criminal court proceedings after forensic analysis (Spasić & Stevanović, 2015, p. 212), experts are therefore not suitable for cross-examination on certain circumstances because from their non-legal point of view there are no ambiguities.

4. Concluding considerations

The use of digital evidence in criminal proceedings, both from the perspective of international legislation and practice and from the perspective of domestic legislation, is neither a novelty nor a negative connotation, even the opposite. Digital evidence can be seen as common jurisprudence in legal systems. Everything is subject to criticism, including digital evidence.

There are significant challenges with digital evidence, especially when considering how it is collected, stored and later forensically processed. Then there is the question of their credibility in terms of whether certain manipulation can be carried out with them and whether it can be detected. It is precisely these questions that present the greatest challenges in terms of the integrity of that evidence. Many other questions can be opened, such as, for example. privacy protection during forensic analysis of digital evidence or during initial access. Of course, to a certain extent, there is also the issue of fear of damage to such data. It would be extremely devastating if special ie. key evidence in criminal proceedings due to any of the above leads to their disqualification as legal evidence. Also, there are concerns about the possibility of excessive surveillance and endangering human rights, as access to digital data may lead to violations of the privacy of suspects or third parties.

If digital evidence is viewed as a balance of law, technique and ethics, then it can be interpreted in criminal proceedings as valid evidence.

The goal of this research was to point out that digital evidence before a criminal court does not and should not have a different status than evidence in a classical material sense, of course under the assumption that digital evidence (just like the so-called classical evidence) has been collected, processed and presented in the manner established by law. The importance of digital evidence is special in the case of crimes related to high-tech criminality, where neither

the criminal process nor the detection of the perpetrators can be imagined without them, and therefore neither can the adoption of a court decision.

Digital evidence can practically be perceived not only as digital data in a physical or cloud environment, but they represent the digital life and movement in the digital world of each of us. Precisely because of the aforementioned, they have a special weight in the broadest sense. Older generations still go "online" while young generations live online.

The special importance of digital evidence and to a certain extent is its affirmation and demystification, even though it has been used for years, which is why regulation 2023/1543 and directive 2023/1544, which were adopted by the EU, are important. The regulation begins to apply from August 18, 2026, and the directive will have to be implemented into domestic legislation by February 18, 2026.

Given the constant advancement of technology, this topic remains crucial for the further development of the justice system in the digital age.

Matijašević Jelena
Univerzitet Privredna akademija u Novom Sadu, Pravni fakultet za privredu i pravosuđe u Novom Sadu, Novi Sad, Srbija

Bingulac Nenad
Univerzitet Privredna akademija u Novom Sadu, Pravni fakultet za privredu i pravosuđe u Novom Sadu, Novi Sad, Srbija

Darko Marinković
Kriminalističko-policijski univerzitet, Beograd, Srbija

DIGITALNI DOKAZI U KRIVIČNOM POSTUPKU – IZAZOVI I REŠENJA

APSTRAKT: Digitalni dokazi u krivičnom postupku poslednje decenije postali su ključni alat u savremenoj forenzičkoj istrazi uz pomoć koje se omogućava identifikacija, analiza i verifikacija informacija koje mogu biti presudne za donošenje odluke u sudskom postupku. Digitalni podaci kroz percepciju raznih oblika elektronskih zapisa, sve više postaju osnovni

dokazi u krivičnim slučajevima, te se zbog toga i ne pravi razlika između dosadašnjih materijalnih dokaza i savremenih digitalnih dokaza. U ovom istraživanju ukazano je i naznačeno na značaj digitalnih dokaza, zatim na njihove prednosti i izazove u prikupljanju i obradama, kao i pravne i etičke aspekte njihove upotrebe u krivičnom postupku. Ukazano je i na značaj metodološkog pristupa u forenzičkoj analizi digitalnih dokaza, a sve kako bi se postigla prihvatljivost digitalnih dokaza pred krivičnim sudom. Kroz celokupno istraživanje provlači se i ukazuje se na izazove i mogućnosti koje ovi dokazi pružaju. Hipoteza ovog istraživanja je sadržana u njegovom naslovu i odnosi se upravo na sporna pitanja i zakonodavnu primenu digitalnih dokaza u krivičnom postupku. Cilj rada je razmatranje ove tematike i kroz sagledavanje nove uredbe i direktive koje su donete a tek će 2026. godine biti usvojene, ali i načelno razmatranje pitanja digitalnih dokaza kroz praksu jer ova tema ostaje ključna za dalji razvoj pravosudnog sistema u digitalnom dobu. Tokom pisanja ovog istraživanja korištena je analitička metoda kao bi se razmotrila legislativa Evropske unije, i načinila komparacija sa domaćim zakonodavstvom. Zatim je korišten normativni metod prilikom razmatranja krivičnopravne procedure i definisanja digitalnih dokaza, kao i deduktivni metod.

Ključne reči: *digitalni dokazi, krivično pravo, krivični postupak, evropska legislativa, forenzička analiza.*

References

1. Bajović, V. (2024). *Zakonik o krivičnom postupku: Neophodno precizirati korišćenje digitalnih dokaza u krivičnom postupku* [*Criminal Procedure Code: It is necessary to specify the use of digital evidence in criminal proceedings*]. Downloaded 2024, October 7 from www.paragraf.rs/dnevne-vesti/221222/221222-vest2.html
2. Budapest Convention (2021). The Convention on Cybercrime. Budapest Convention, ETS No. 185 and its Protocols
3. Camp, S. (2024). *Online Shopping Security Issues and How Cyber Security can Help.* Downloaded 2024, October 7 from www.ecpi.edu/blog/online-shopping-security-issues-and-how-cyber-security-can-help
4. Casey, E. (2004). *Digital Evidence and Computer Crime.* Waltham: Academic Press
5. Committee, C. C. (2020). *The Budapest Convention on Cybercrime – benefits and impact in practice.* Strasbourg: Council of Europe

6. Cybercrime (2024). Retrieved from 20th anniversary Budapest Convention – Benefits, Downloaded 2024, October 7 from www.coe.int/en/web/cybercrime/benefits
7. Convention on Cybercrime (2024). *Joining the Convention on Cybercrime: Benefits.* Council of Europe
8. Councle of Europe (2001). *European Treaty Series – No. 185 – Convention on Cybercrime*
9. Champlain College (2024). The Evolution of Digital Forensics. Retrieved from Champlain College Online: Downloaded 2024, October 7 from https://online.champlain.edu/blog/evolution-digital-forensics
10. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings
11. Directive (EU) 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings
12. Iproceeds (2024). Izveštaj o proceni u vezi sa pribavljanjem i korišćenjem elektronskih dokaza u krivičnom postupku na osnovu domaćeg zakonodavstva u zemljama jugoistočne Evrope i Turskoj. [Assessment report regarding the acquisition and use of electronic evidence in criminal proceedings based on domestic legislation in Southeast European countries and Turkey]. *Project on targeting crime proceeds on the Internet in South-East Europe and Turkey*. Downloaded 2024, October 7 from https://rm.coe.int/3156-52-iproceeds-electronic-evidence-report-serbian/16807bdfe3
13. Juszczak, A., & Sason, E. (2023). The Use of Electronic Evidence in the European Area of Freedom, Security, and Justice. *EuCrim,* (2), pp. 182–200
14. Kovačević, M. (2013). Video nadzor na javnim mestima i pravo na privatnost [Video surveillance in public places and the right to privacy]. *Teme, 37*(4), pp. 1795–1810
15. Krivični zakonik [Criminal code]. *Službeni glasnik RS*, br. 85/05, 88/05 – ispr., 107/05 – ispr., 72/09, 111/09, 121/12, 104/13, 108/14, 94/16, 35/19 i 94/24.
16. Macan, S. (2021). Pravna prihvaljivost nivoa bezbjednosti sistema elektronske identifikacije [Legal acceptability of the security level of the electronic identification system]. *Godišnjak Fakulteta pravnih nauka, 11*(11), pp. 186–199

17. Matijašević, J. (2012). Visokotehnološki kriminal u funkciji organizovanog kriminaliteta [High-tech crime in the function of organized crime]. In: Bjelac Ž., & Zirojević, M. (ur.), *Organizovani kriminalitet – izazov XXI veka* [*Organized Crime – The Challenge of XXI century*] (pp. 398–420). Novi Sad: Pravni fakultet za privredu i pravosuđe u Novom Sadu, Univerzitet Privredna akademija u Novom Sadu
18. Mihajlović, A. (2024). *Zakonik o krivičnom postupku – neophodno precizirati korišćenje digitalnih dokaza u krivičnom postupku* [*Criminal Procedure Code – It is necessary to specify the use of digital evidence in criminal proceedings*]. Downloaded 2024, October 7 from www.paragraf.rs/dnevne-vesti/221222/221222-vest2.html
19. Miljuš, I. (2024). *Zakonik o krivičnom postupku – neophodno precizirati korišćenje digitalnih dokaza u krivičnom postupku* [*Criminal Procedure Code – It is necessary to specify the use of digital evidence in criminal proceedings*]. Downloaded 2024, October 7 from www.paragraf.rs/dnevne-vesti/221222/221222-vest2.html
20. University of Oxford. *Information Security – Protect my privacy online*. Downloaded 2024, October 7 from www.infosec.ox.ac.uk/protect-my-privacy-online
21. Osco, M., Mercedes, C., Quinones, A., & Joaquin, D. (2024). Digital Evidence as a Means of Proof in Criminal Proceedings. *Revista de Gestão Social e Ambiental, 18*(4), pp. 1–13
22. Petrović, L. (2004). *Digitalni dokazi* [*Digital evidence*]. Ziteh, pp. 1–13. Downloaded 2024, October 7 from https://singipedia.singidunum.ac.rs/izdanje/40058-digitalni-dokazi
23. Propp, K. (2024). *CBDF.* Retrieved from LAWFARE – Navigating Toward an EU-U.S. Agreement on Electronic Evidence: Downloaded 2024, October 7 from www.crossborderdataforum.org/lawfare-navigating-toward-an-eu-u-s-agreement-on-electronic-evidence/
24. Ragni, C. (2023). Digital evidence in international criminal proceedings and human rights challenges. *International Scientific Conference on International, EU and Comparative Law Issues "Law in the Age of Modern Technologies"*, *7*, pp. 1–16
25. Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings.
26. Reith, M., Carr, C., & Gunsch, G. (2003). An Examination of Digital Forensic Models. *International Journal of Digital Evidence, 1*(3), pp. 1–9

27. Spasić, V., & Stevanović, B. (2015). Dokazivanje digitalnih povreda prava intelektualne svojine – osvrt na anglosaksonski pravni sistem [Proving digital violations of intellectual property rights – a review of the Anglo-Saxon legal system]. *Zbornik radova Pravnog fakulteta u Nišu, 54*(69), pp. 203–226
28. Sulcas, A. (2024). *What is Targeted Marketing? Definition, Strategies & Examples*. Downloaded 2024, October 7 from www.sender.net/blog/targeted-marketing/
29. Tompkins, J., & Mar, L. (1986). The 1984 Federal Computer Crime Statute: A Partial Answer to a Pervasive Problem, 6 Computer L.J. 459 (1986). *UIC John Marshall Journal of Information Technology & Privacy Law, 6*(3), pp. 461–482
30. Wahl, T. (2023). E-evidence Regulation and Directive Published. *EuCrim*, pp. 165–168.
31. Zakonik o krivičnom postupku [Criminal Procedure Code], *Službeni glasnik RS*, br. 72/11, 101/11, 121/12, 32/13, 45/13, 55/14, 35/19, 27/21 – odluka US i 62/21 – odluka US