III

CURRENT TRENDS IN CRIMINAL LAW

UDC: 347.93:004
DOI: 10.5937/PDSC25370V

Academician Prof. Dr Branko Vučković, Professor Emeritus
Adriatic University – Faculty of Business Economics and Law, Bar
President of the Association for Criminal Law and Criminal Policy of Montenegro

Academician Prof. Dr Vesna Vučković
Adriatic University – Faculty of Mediterranean Business Studies, Tivat
In Kotor, Montenegro, 5th May 2025
e-mail: bvvuckovic@gmail.com

DIGITAL EVIDENCE IN COURT PROCEEDINGS
– Between Law and Justice –

Abstract:

Digital evidence represents any information that has evidential value, can be transmitted electronically, and stored. Information technologies are rapidly evolving and significantly altering the way communication is conducted. In professional literature, various definitions of digital evidence exist. Today, computers are increasingly being used as either the instrument or the target of criminal offences. Therefore, in the combat against modern forms of crime, knowledge of digital evidence is essential, along with the existence of specific rules and procedures for its detection and collection by information technology experts. Digital forensics deals with digital evidence and is based on the principle of legality – meaning that digital evidence may only be collected on the basis of a court order. Key issues include: who is responsible for the right to privacy? How can one determine whether there is an overriding interest that justifies the use of digital evidence obtained without the person's knowledge? In other words, does this constitute a violation of the right to privacy? This paper will underscore the significance of digital evidence in court proceedings, with reference to the opinions and case law of the European Court of Human Rights.

Keywords: *digital evidence, legality, collection, assessment, European Court of Human Rights.*

INTRODUCTION

Today, in modern society, computers are an indispensable tool that has completely changed the way we work, creating new forms of labour. Although they have many advantages when used for "positive" purposes, they also have their downsides when used to commit criminal acts.

Modern forms of crime, due to their specific methods of execution and the use of signs in a technological sense, are difficult to prove, especially because of the involvement of Internet providers and many other relevant authorities.

The fight against modern forms of crime, especially those in which computers are used as a means or object of the crime, requires knowledge of digital evidence, particularly regarding procedures for its detection, documentation, and collection.

The presentation of digital evidence in court proceedings is an essential part of crime detection and prosecution. In this regard, it is important to know and use computer forensics, which is a *conditio sine qua non* (an essential condition) for uncovering digital evidence and presenting it in legal proceedings.

Digital evidence today occupies an increasingly important place in the prosecution of criminal acts.

THE CONCEPT OF DIGITAL EVIDENCE

In professional literature, various definitions of the term digital evidence can be found.

The most commonly cited definitions are:

*Any data stored or transmitted using a computer that supports or refutes a theory of how an offense occurred, or that addresses critical elements of a criminal act, such as intent or alibi.[1]

*Digital evidence is a broad term used to describe any record generated by, or stored on, a computer system that can be used as evidence in a court proceeding.[2]

*All information of evidentiary value stored or transmitted in digital form.[3]

*Information or data, stored or transmitted in binary form, that can be used as evidence.[4]

The terms digital and electronic evidence are used interchangeably.

They can generally be classified into three categories:

(I) records that are computer-stored,

(II) computer-generated records, and

(III) records that are partially computer-generated and partially computer-stored.[5]

1 E. Casey (2004), Digital Evidence and Computer crime, Second Edition, Academic Press, p. 40

2 HB 171 (2003), Guidelines for the management of IT evidence, p. 9

3 SWGDE and SWGIT, Digital & Multimedia Evidence Glossary, p. 19

4 Information technology-Security techniques-Guidelines for indetification, collection, acquisition and preservation of digital evidence, p. 24

5 HB 171 (2003), Guidelines for the management of IT evidence, p.12

Digital evidence is defined as any data presented in electronic form and obtained in accordance with the law for use as evidence.[6]

Digital evidence must be obtained in accordance with the law; otherwise, it is considered inadmissible in court proceedings.

It can be found in various places, including user devices—laptops, mobile phones, digital cameras, etc. However, digital evidence also includes address books, e-mails, files, and similar data. Digital evidence refers to data that includes sounds, images, and traffic through various forms of communication.

Despite the broad definition of digital evidence, it is essential that its handling in court proceedings be conducted in a way that withstands judicial scrutiny. Only in such cases can it be used in legal proceedings, as digital evidence presents significant challenges in order to be considered legally valid. It is not uncommon for concerns to arise about its reliability, bearing in mind that original content can easily be destroyed, altered, or damaged, which may lead to various forms of manipulation.

LEGAL FRAMEWORK FOR THE USE OF DIGITAL EVIDENCE

The Criminal Code of Montenegro[7] defines, in accordance with the Convention on Cybercrime[8], pojam računarski sistem, podatak i p the terms computer system, data, and program.

A computer system is considered to be any device or group of interconnected or interdependent devices, one or more of which, depending on the program, performs automatic data processing.

A computer data is considered to be any representation of facts, information, or concepts in a form suitable for processing in a computer system, including programs through which the computer system performs its functions.

A computer program is considered to be a set of organized computer data based on which the computer system performs its functions.

The Criminal Code prescribes criminal offenses related to this matter in Chapter XXVIII – Criminal Offenses Against the Security of Computer Data (Articles 349–354).

The Criminal Procedure Code of Montenegro[9] regulates the use of electronic data in various ways—both individually and interconnected—that are automatically processed based on programs. A wide range of devices that operate on the principle of automatic data processing are considered to be computers. For the purpose of proving a criminal offense, a search of computers and computer equipment is almost always conducted.

6 Š. Pavlović, (2017), Criminal Procedure Code, Third significantly amended, supplemented, and expanded edition, Libertin Publishing, Rijeka, p. 551

7 Criminal Code of Montenegro, "Official Gazette of the Republic of Montenegro," no. 70/03 … "Official Gazette of Montenegro," no. 40/08 … 123/24

8 Convention on cybercrime in the criminal, signed in Budapest on 23 November 2001

9 Criminal Procedure Code of Montenegro, "Official Gazette of Montenegro," no. 57/09 … 54/24

DIGITAL EVIDENCE AND THE EUROPEAN UNION

The European Union is continuously developing and improving cross-border access to digital evidence in criminal cases with the aim of enhancing access to such evidence, while establishing a legal framework for court orders that are directly addressed to legal representatives of service providers, without the involvement of authorities from the member state where the legal representative is located. This was done through the adoption of 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, as well as the Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings.

According to these documents, anyone wishing to provide services within the European Union is obligated to cooperate with investigative bodies based on the principle of mutual trust. However, these proposals do not cover "direct access to e-evidence" and "real-time data interception".

The Proposal for a Regulation of the European Parliament and of the Council on the European Production Order and the European Preservation Order for electronic evidence in criminal matters provides for the use of specific, standardized forms—namely, the European Production Order Certificate (EPOC) and the European Preservation Order Certificate (EPOC-PR). According to this regulation, both orders must be confirmed or issued by the judicial system of a member state to secure or provide information held by a service provider from another jurisdiction, which is needed as evidence in a criminal investigation or criminal proceeding. Both orders may be served to providers of electronic communications services, state networks, websites, and other roaming and web infrastructure service providers, such as IP address registries and domain name registries, or to their legal representatives, if such exist.[10]

The European Preservation Order, like the European Production Order, applies to both identified and unidentified perpetrators of criminal offenses and concerns evidence that has already been obtained. The proposal includes safeguards, such as: - it does not apply to real-time interception of telecommunications; - the measure is limited to what is necessary and proportionate to the objectives of the specific criminal proceedings; - it allows service providers to request clarification from the issuing authority, if needed.

The Proposal for a Directive of the European Parliament and of the Council on establishing harmonized rules for the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings[11] arose from the need to address the differing approaches taken by member states regarding the obligations imposed on service providers in criminal proceedings. These differing approaches could lead to legal uncertainty. Therefore, an obligation was introduced to appoint a legal representative within the Union who will receive, acknowledge, and enforce decisions issued by the competent national authorities for the purpose of collecting digital evidence, especially in criminal proceedings.

10 H. Sijarčić, H. Halilović (2020), *Digital Evidence and the Modern Criminal Procedure*, *Legal Thought*, no. 9–10, Sarajevo, p. 86.

11 Retrieved from https://eur-lex.europa.eu/legal-content/SL/ALL,uri COM%/AFIN, on 18 May 2025

DIGITAL EVIDENCE AND THE EUROPEAN COURT OF HUMAN RIGHTS

The European Convention on the Protection of Human Rights[12] does not contain specific provisions related to digital evidence, although the case law of the European Court of Human Rights has had to deal with such evidence, the particularities of its collection and use, especially ensuring that it does not lead to violations of guaranteed human rights and freedoms.

From the Court's perspective, it is especially important to determine how digital evidence was collected, its evidentiary value, how it is used, and whether it can serve as a basis for a conviction.

a) Collection of Evidence

Digital evidence can be collected in various ways, including through search and seizure warrants or based on surveillance measures, such as the interception of communications, audio and video recording, and the use of tracking devices. If there is no consent for this method of collection, a violation of Article 8 of the European Convention may be raised. This article states, among other things, that everyone has the right to respect for their private and family life, home, and correspondence. Public authorities may interfere with the exercise of this right only if it is in accordance with the law and necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention of disorder or crime, protection of health or morals, or protection of the rights and freedoms of others.

Evidence may also be collected based on the consent or approval of the individual. The consent must be voluntary and not of such a nature that the person giving it felt there was no other option but to allow access.

Evidence collection is also possible without the person's consent, but only in cases where it is necessary in a democratic society and in the interest of national security. In all cases, there must be a legal basis for the collection; otherwise, it constitutes a violation of Article 8 of the Convention.

The collection and processing of digital evidence is handled by computer forensics, which operates under the *principle of legality*, meaning that collection is carried out only on the basis of a court order, and also under the chain of custody, meaning that one piece of digital evidence must not exclude another.

b) Evidentiary Value

According to the European Court, digital evidence can be important when determining whether certain facts can be considered established (either in proceedings before national courts or in proceedings before the European Court of Human Rights). Such facts relate to questions such as - *whether specific individuals were at a particular place at the time of a given event* (e.g., when phone data indicates the whereabouts of individuals at the time of an alleged poisoning)[13]; *whether there was complicity in certain behavior or events* (e.g., video footage shows police facilitating an attack against certain protesters during a demonstration)[14]*; whether the behavior of the accused constituted a criminal offense*

12 European Convention on Human Rights, adopted in Rome on November 4, 1950

13 *Application Navalnyy v. Russia,* no. 36418/20 dated 6 June 2023

14 *Application Women's Initiatives Support Group and Others v. Georgia,* no. 73204/13, dated 16 December 2021

(e.g., video footage shows the accused loading drugs into a car)[15]; *whether the person resisted during arrest* (e.g., video footage shows the police threatening to break the accused's arm if he does not stay still, after stepping on his feet until entering the police station)[16]; *determining how certain consequences occurred* (e.g., the use of satellite imagery to establish whether houses were destroyed by fire or by bombing)[17].

GUARANTEES AND VALIDITY OF DIGITAL EVIDENCE

Digital evidence shall be considered valid and lawful if the principle of equality of arms is respected, and if access is not denied to documents that are necessary for establishing the facts of the case.

The European Court has taken the position that where evidence is very strong and there is no risk of it being unreliable, the need for corroboration with other material evidence is reduced.[18] The court must properly assess the evidentiary value of each piece of digital evidence presented before making a decision.

European Court has not found that relying on electronic evidence to render a conviction, in situations where such evidence was collected without a basis in national law, automatically leads to an unfair trial, in cases such as:

*recordings of telephone conversations (*Schenk v. Switzerland*, no. 10862/84, dated 12 July 1988)

*use of listening devices to record conversations (*Khan v. the United Kingdom*, no. 35394/97, dated 12 May 2000)

*creating video recordings (*Perry v. the United Kingdom*, no. 63737/00, dated 26 September 2002)[19]

PRIVACY AND THE USE OF INFORMATION TECHNOLOGY

Privacy is one of the fundamental human rights. The development of new information technologies has led to the creation of systems that enable mass surveillance, monitoring, and wiretapping. The global electronic communication system has become a source of a wide variety of data about individuals. The development of electronic communications raises numerous issues, primarily the protection of citizens' rights to privacy. The issue of privacy has become especially relevant with the use of information and communication technologies and electronic communications.

15 *Application Fejzula and Mazreku v. the Former Yugoslav Republic of Macedonia,* no. 23065/07, dated 31 May 2011

16 *Application Navalnyy and Gunko v. Russia,* no. 75186/12, dated 10 November 2020

17 *Application Georgia v. Russia (II) [GC],* no. 38263/08, dated 21 January 2021

18 *Application Basak and others v. Croatia,* no. 40429/14 dated 6 June 2019

19 Handbook, Case Law of the European Court of Human Rights on the Use of Electronic Evidence (2024), European Union and Council of Europe, p. 40

The threat posed by technology, and thus to privacy, increases with the use of the Internet, which has both advantages and weaknesses.

Today, the question is often raised whether the disclosure of so-called 'encrypted communication' infringes upon the privacy of individuals whose communication has been revealed, especially in cases involving the commission of serious criminal offenses by criminal organizations.

As early as 2016, investigative authorities in Belgium determined that criminal organizations were using encrypted communication via specially created devices and networks ("Ennet coni"), while in 2020, French police authorities decrypted the "Encro Chat" network. Since then, the United States, Australia, the Netherlands, and Belgium have discovered and decrypted communications on Sky ECC and ANOM.

The documentation of encrypted communication between members of criminal groups constitutes significant evidentiary material, provided that such evidence is obtained in a manner and under the conditions prescribed by the Criminal Procedure Code. In Montenegro, judicial authorities are conducting criminal proceedings in which the contents of encrypted communications—primarily Sky ECC—have been submitted as evidence. In such cases, certain judicial decisions have already been rendered, including those concerning the imposition and extension of detention, as well as judgments, although such judgments have not yet become final.

The Canadian communication network Sky Global provided service as a provider, and its most notable products included the Sky ECC messaging application. ANOM is a telecommunications company that developed mobile devices with only one functional application, which was pre-installed and used exclusively for encrypted messaging. These devices lacked all other features typical of modern smartphones.

Considering that these communications were used to commit the most serious criminal offenses by criminal organizations, it is considered that individuals in such cases cannot invoke a violation of the right to privacy, as the prevailing interest lies in uncovering serious criminal offenses.

Criminal groups and organizations have demonstrated significant flexibility in "the use of telecommunications technologies", which has enabled their unlimited networking and connectivity. The identity of users has been protected through *interface* encryption (concealing it to the point of being undetectable), as well as through registration and usernames, which are typically pseudonyms or nicknames. Believing that communication over encrypted networks could not be intercepted, members of criminal organizations communicated completely openly, coordinating and planning the commission of criminal offenses, often providing confirmation in the form of recordings (videos or images, photographs), including the most serious criminal offenses—such as murders, torture, and others.[20]

Believing that their devices were protected from surveillance, members of criminal groups openly talked and exchanged messages regarding the planning and execution of criminal acts.

20 C. Osborne (2016), Dutch police close Ennetom encrypted communications network, https://www.zdnet.com/article/dutch-police-arrest-ownwr-of-ennetcom-encryption-network, accessed on 21 May 2025

LEGALITY OF EVIDENCE OBTAINED THROUGH "ENCRYPTED COMMUNICATION"

The obtaining of electronic-digital evidence from "encrypted communication" raises certain questions, primarily due to the manner in which the evidence is obtained and the source from which it originates.

When deciding on the legality and admissibility of evidence, the method of its acquisition must be known.

According to Article 17 of the Criminal Procedure Code, among other things, it is prohibited to base a court decision on evidence obtained by violating human rights and freedoms prescribed by the Constitution and confirmed by international treaties.

The central issue is the legality of the way data was transmitted to another country, since encrypted communication (digital evidence) is a document obtained through international legal assistance. Namely, there is no other way to obtain this evidence except through international legal assistance. Therefore, the assessment of the admissibility of evidence obtained abroad is of crucial importance.

The legal assessment of the authenticity and reliability of digital evidence depends on the chosen digital forensic process, methods, and tools for each forensic task, as well as the chain of custody of the collected data, which can demonstrate the preservation of data integrity and reliability.[21]

The quality of evidence must be taken into account, which implies considering whether the circumstances under which the evidence was obtained raise suspicion regarding its reliability or accuracy.[22]

CONCLUSION

Digital evidence is a type of evidence that differs from other evidence by the form in which the information is incorporated — a digital form. However, in terms of its value, this evidence is equated with physical evidence, although its collection requires special equipment.

Digital evidence is a modern form of evidence that is increasingly used in court proceedings, especially in the prosecution of criminal offenses and their perpetrators. Although legal regulations recognize the possibility of using digital evidence to prove relevant facts in the proceedings, certain difficulties still exist, particularly regarding the framework for its collection—temporary seizure of items, searches, expert examinations, and others.

The lawful acquisition of digital evidence is crucial for its use. Such evidence can be found in various places, including a wide network of usage, and even through "encrypted" communication among members of organized criminal groups. These arise from the process of mass surveillance of an unspecified number of users of this type of communication.

21 R. Stoykova (2022), Encrochat: The Hacker with a Warrant and Fair Trails, p.4

22 *Application Allan v. the United Kingdom*, App.N.48539/99 dated 5 February 2003, para. 43

The use of such evidence in court proceedings is a topic that requires special consideration of procedures to ensure authenticity and integrity.

With this type of evidence, the issue of protecting human rights, particularly privacy, arises. Guarantees for the protection of human rights and fundamental freedoms must be respected, and international standards must be ensured in their protection.

The European Convention on Human Rights does not contain specific provisions related to digital evidence, although case law has had to address this issue due to the specific nature of its collection and use, ensuring that its acquisition and use do not lead to unjustified interference with guaranteed rights and freedoms.

International cooperation is of particular importance regarding the access, exchange, and use of digital data. Therefore, the harmonization of norms with other countries represents a *conditio sine qua non* for the success of discovering and proving, as well as using, such digital evidence obtained in this way.

Considering the rapid development of information technology, it is necessary that positive legal regulations keep pace with this development in accordance with international standards.

Akademik prof. dr Branko Vučković, prof. emeritus
Univerzitet „Adriatik"-Fakultet za poslovnu ekonomiju i pravo Bar
Predsjednik Udruženja za krivično pravo i kriminalnu politiku Crne Gore

Akademik prof. dr Vesna Vučković
Univerzitet „Adriatik"-Fakultet za mediteranske poslovne studije Tivat
Kotor, Crna Gora, 05.maj 2025. godine
e-mail: bvvuckovic@gmail.com

DIGITALNI DOKAZI U SUDSKOM POSTUPKU
-između prava i pravde-

Apstrakt:

Digitalni dokaz je svaka informacija koja ima dokaznu vrijednost, koja se može prenijeti u elektronskom obliku i uskladištiti. Informacione tehnologije iz dana u dan ubrzano se razvijaju i radikalno utiču na izmjenu načina na koji se komunicira. U stručnoj literaturi postoje različite definicije digitalnih dokaza. Danas se računari sve češće pojavljuju kao sredstvo ili predmet izvršenja krivičnog djela, pa u borbi protiv savremenih oblika kriminaliteta nužno je poznavanje digitalnog dokaza uz postojanje posebnih pravila i procedura u njihovom otkrivanju i prikupljanju od strane stručnjaka informacione tehnologije.Digitalnim dokazima bavi se digitalna forenzika koja za osnovu ima princip zakonitosti-mogućnost prikupljanja digitalnih dokaza isključivo na osnovu odluke suda.

Ključno pitanje je,ko je odgovoran za pravo na privatnost, kako utvrditi pretežniji interes da se digitalni dokaz koji je pribavljen bez znanja tog lica može koristiti, odnosno, da li se radi o povredi prava na privatnost. U radu će se ukazati na značaj digitalnih dokaza u postupcima pred sudom, sa osvrtom na stavove i praksu Evropskog suda za ljudska prava.

Ključne riječi: *digitalni dokaz, zakonitost, pribavljanje, ocjena, Evropski sud za ljudska prava.*

REFERENCES

1. E. Casey (2004), Digital Evidence and Computer crime, Second Edition, Academic Press
2. C. Osborne (2016), Dutch police close Ennetom encrypted communications network,
3. Š. Pavlović, (2017), Law on Criminal Procedure, Third significantly amended, supplemented, and expanded edition, Libertin Publishing, Rijeka
4. H. Sijarčić, H. Halilović (2020), *Digital Evidence and Modern Criminal Procedure*, Pravna misao, No. 9-10, Sarajevo
5. R. Stoykova (2022), Encrochat: The Hacker with a Warrant and Fair Trails
6. Criminal Code of Montenegro, Official Gazette of RCG, No. 70/03 … Official Gazette of Montenegro, No. 40/08 ….123/24
7. Criminal Procedure Code of Montenegro, Official Gazette of Montenegro, No. 57/09 … 54/24
8. European Convention on Human Rights
9. Convention on Cybercrime
10. Information technology-Security techniques-Guidelines for indetification, collection, acquisition and preservation of digital evidence
11. HB 171 (2003), Guidelines for the management of IT evidence
12. SWGDE and SWGIT, Digital &Multimedia Evidence Glossary
13. HB 171 (2003), Guidelines for the management of IT evidence
14. Manual, *Case Law of the European Court of Human Rights on the Use of Electronic Evidence* (2024), European Union and Council of Europe

Case Law of the European Court of Human Rights

15. *Application Navalnyy v. Russia*, no. 36418/20 dated 6 June 2023
16. *Application Group for Support of Women's Initiatives and Others v. Georgia*, no. 73204/13 dated 16 December 2021
17. *Application Fejzula and Mazreku v. the Former Yugoslav Republic of Macedonia*, no. 23065/07 dated 31 May 2011
18. *Application Navalnyy and Gunko v. Russia*, no. 75186/12 dated 10 November 2020
19. *Application Georgia v. Russia* (II) GC, no. 38263/08 dated 21 January 2021
20. *Application Basak and others v. Croatia*, no. 40429/14 dated 6 June 2019
21. *Application Allan v. the United Kingdom*, App. No. 48539/99 dated 5 February 2003, para. 43

Websites

1. https://eur-lex.europa.eu/legal-content/SL/ALL,uri COM%/AFIN
2. https://www.zdnet.com/article/dutch-police-arrest-ownwr-of-ennetcom-encryption-network