

*Davor TRLIN**

International Burch University Sarajevo

*Ajla BAŠIĆ***

Center for judicial and prosecutorial training of the Federation of BiH

KEY ASPECTS OF THE IMPACT OF THE CONSTITUTIONALITY OF DIGITAL EVIDENCE ON THE EFFICIENCY OF CRIMINAL JUDGMENTS

The legal system must adapt to rapidly evolving technologies, balancing human rights protection, particularly privacy and fair trial rights, with efficient crime prevention. Digital evidence collection requires constitutional compliance, such as obtaining search and interception warrants, while ensuring confidentiality and dignity. A key challenge is maintaining the authenticity of digital evidence through a proper chain of custody and technical expertise to prevent alteration. Digital evidence enhances criminal justice efficiency by enabling rapid data collection and analysis, but challenges like data overload and statutes of limitations persist. The rights of the accused, including defense and presumption of innocence, must be upheld in digital cases amidst global issues like inter-jurisdictional data access and international treaty compliance. This paper examines how digitization has driven global legal systems to adopt digital evidence, highlighting authentication challenges and the need for Bosnian and Herzegovinian legislators to revise laws based on the European Court of Human Rights and Constitutional Court jurisprudence. Through case studies from Bosnian and Herzegovinian courts and prosecutors' offices, the paper illustrates both effective and problematic practices in handling digital evidence.

Keywords: Digital evidence, IT expertise, criminal justice, constitutionality, jurisprudence.

1. INTRODUCTION

Accelerated globalization and digitalization bring benefits but also challenges in managing personal data, raising concerns about privacy, security, and misuse as digital evidence. States must critically review regulations to balance societal interests with individual rights and freedoms. It is not uncommon for legal regulations not to keep up with this accelerated development of technologies, and for legal norms and regulations, which should be the basis for establishing standards for protecting personal data, to be quite incomplete and outdated.

* PhD, Associate Professor, ORCID: orcid.org/0000-0001-6118-9757, e-mail: davor.trlin@ibu.edu.ba

** LLM, Professional associate, ORCID: [0009-0005-0055-1034](https://orcid.org/0009-0005-0055-1034), e-mail: ajla.basic@cest.gov.ba

This results in an inadequate definition of digital evidence, and a lack of practical experience in the proper collection, processing and preservation of this type of evidence, ultimately threatening to undermine the balance between security and privacy and thereby potentially violating the rights and freedoms guaranteed by the Constitution and the European Convention on Human Rights (ECHR) and its protocols.

Different states have established different legal mechanisms for collecting evidence in criminal proceedings, as well as different approaches to what is considered illegal evidence and how it is treated. In this context, the definition of the concept of illegal evidence varies in different legal systems and legal definitions.

Because of these differences, it would be almost impossible for the European Court for the Human Rights (ECtHR) to establish uniform standards applicable to all legal systems of the member states, which would lead to imposing certain rules on national legislation. Therefore, it is logical to leave the regulation of this institute to national legislation. By comparing the amended legal solutions, it can be concluded that they are not mutually harmonized and that they differ both in terms of the (seriousness) of the criminal offenses for which special investigative measures can be ordered, and in terms of the deadlines for their implementation.

The practice of the European Court of Justice in relation to special investigative measures, and in this context, the use of illegally obtained evidence and the quality of the law, is extremely rich. However, what is common to this entire practice is the standards and general principles established by the ECtHR and which should be adhered to (Knežević & Dumanjić, 2019, p. 83).

The largest number of applications submitted to the ECtHR are those in which the appellants point to the illegality of evidence within the meaning of Articles 6 and 8 of the ECHR obtained through the application of special investigative measures.

Numerous decisions that the Constitutional Court of BiH has made within the appellate jurisdiction confirm the importance of constitutional protection of fundamental human rights and freedoms in criminal proceedings when applying special investigative measures (Adžajlić Hodžić *et al.*, 2021, p. 19), taking positions on certain issues and creating case law as a “guide” for the actions of regular courts, which, referring to the jurisprudence of the Constitutional court of BiH and the ECtHR, also take on the important role of guarantor/protector of the right to privacy and fair trial, and ultimately contribute to harmonizing the norms and practice of court proceedings with the Constitution of BiH, international standards of the ECHR and the practice of the ECtHR.

In the context of Article 8 of the ECHR and the examination of its violation, in many decisions of the ECtHR, but also the Constitutional court of BiH, have determined that the use of special investigative measures constitutes interference with the right to private life, home and correspondence, whereby this right guaranteed by the ECHR (and to which the rights and freedoms guaranteed by Article II/3.f) of the Constitution of BiH correspond), is viewed as a qualified convention right. This definition implies the freedom of the state to interfere with the exercise of this right, and the C explicitly states when such interference is to be considered necessary/justified.¹

¹ See: Art. 8, para. 2 of the ECHR - the right to respect for private and family life. Available on: https://www.echr.coe.int/documents/d/echr/convention_bos (28. 3. 2025).

Whether such interference by the competent authorities serves a legitimate aim will be assessed from the circumstances of each specific case, whereby it is understood that the law should contain guarantees against misuse, ie, precisely prescribe the discretionary powers of the competent authorities. Therefore, the law that prescribes the implementation of these actions must be sufficiently clear so that the individual is aware of "*in what circumstances and under what conditions public authorities have the authority to resort to such measures*".² The competent authorities are obliged to fully respect the procedure prescribed by law, i.e., the standards of the ECtHR and the Constitutional Court, in terms of the legality of the interference, examining whether there are legitimate aims for determining these actions and whether taking these actions is "necessary in a democratic society".³

The Constitutional Court of Bosnia and Herzegovina, in Decision No. U 5/16 on June 1, 2017, declared item d) of Article 117 and paragraph 3 of Article 118 of the Criminal Procedure Code unconstitutional for violating Article I/2 and Article II/3.f) of the BiH Constitution. It was found that Article 117 disproportionately interfered with privacy rights, lacking the strict necessity to protect democratic institutions, while Article 118 failed to differentiate applicable criminal offenses and used a vague criterion of "particularly important reasons". Amendments to the criminal procedure laws addressing these issues were made between September 2018 and February 2021.⁴

2. PROTECTION OF THE RIGHT TO PRIVACY AND CONSTITUTIONAL GUARANTEES

The right to privacy is a universally accepted human right. Basic privacy protection standards are already defined by the United Nations Universal Declaration of Human Rights, as well as the ECHR and its protocols, which directly apply in Bosnia and Herzegovina and have priority over all other laws.⁵ In July 2004, Bosnia and Herzegovina ratified the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its amendments (of June 15, 1999) and the Additional Protocol to the Convention (of November 8, 2001). The Constitutions of Bosnia and Herzegovina, the Federation of Bosnia and Herzegovina, and Republika Srpska guarantee

² *Dragojević v. Republic of Croatia*, European Court of Human Rights, Application no. 68955/11, Judgment of 15. 1. 2015, para. 81

³ *Szabó and Vissy v. Hungary*, European Court of Human Rights, Application no. 37138/14, Judgment of 12. 1. 2006.

⁴ Criminal Procedure Code of Bosnia and Herzegovina, *Official Gazette of Bosnia and Herzegovina*, no. 3/03, 32/03, 36/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 12/09, 16/09, 93/09, 72/13, 65/18; Criminal Procedure Code of the Brčko District of Bosnia and Herzegovina, *Official Gazette of the Brčko District of Bosnia and Herzegovina*, no. 34/2013 - consolidated text and 27/2014; Law on Amendments to the Criminal Procedure Code of the Federation of Bosnia and Herzegovina, *Official Gazette of the Federation of Bosnia and Herzegovina*, no. 74/20; The Law on Amendments to the Criminal Procedure Code of the Republika Srpska, *Official Gazette of the Republika Srpska*, no. 66/18 and the Law on Amendments to the Criminal Procedure Code of the Republika Srpska, *Official Gazette of the Republika Srpska*, no. 15/21.

⁵ Art. II/2 of the Constitution of Bosnia and Herzegovina, Aneks IV Opšteg okvirnog sporazuma za mir u Bosni i Hercegovini and *Official Gazette of Bosnia and Herzegovina*, no. 25/2009 – Amendment I.

the right to privacy, encompassing personal and family life, home, and correspondence for all persons within their respective territories.⁶

Protection of the right to privacy and family life, home, and correspondence is one of the fundamental rights, the realization of which is a prerequisite for the proper functioning of every democratic society.

It is clear from the provisions of all the above-mentioned documents that this right can be broken down into three basic segments, namely:

- private life;
- family life;
- home; and
- correspondence.

When it comes to protecting the right to privacy, the practice of the ECtHR had the most important influence on the creation of internationally recognized standards. According to the opinion of the ECtHR, private life represents a broad concept, which is impossible to give a final definition.⁷

In general, the practice of the court has led to the expansion of the concept of privacy to:

1. physical and moral integrity of the person;
2. collection of data required by the state;
3. access to personal information;
4. regulating names and surnames.⁸

3. LEGAL CERTAINTY AND RELIABILITY OF EVIDENCE

Legal certainty ensures a stable, predictable legal system with consistent law application, allowing individuals to anticipate legal consequences. Reliability of evidence, rooted in its legality, is vital for fair trials, enabling courts to make just decisions based on lawfully collected evidence. Together, they prevent unfounded judgments and uphold fairness in legal proceedings.

⁶ See: Article II/3f of the Constitution of Bosnia and Herzegovina, Aneks IV Opšteg okvirnog sporazuma za mir u Bosni i Hercegovini and *Official Gazette of Bosnia and Herzegovina*, no. 25/2009 – Amendment I.; article II/A2 of the Constitution of the Federation of Bosnia and Herzegovina, *Official Gazette of the Federation of Bosnia and Herzegovina*, no. 1/1994, 1/1994 - Amendment I, 13/1997 - Amendments II-XXIV, 13/1997 - Amendments XXV and XXVI, 16/2002 - Amendments XXVII-LIV, 22/2002 - Amendments LVI-LXIII, 52/2002 - Amendments LXIV-LXXXVII, 60/2002 – correction of the Amendment LXXXI, 18/2003 - Amendment LXXXVIII, 63/2003 - Amendments LXXXIX-XCIV, 9/2004 - Amandmani XCV-CII, 32/2007 - correction 20/2004 - Amendments CIII and CIV, 33/2004 - Amendment CV, 71/2005 - Amendments CVI-CVIII, 72/2005 - Amendment CVI, 88/2008 - Amendment CIX, 79/2022 - Amendments CX-CXXX, 80/2022 – correction and 31/2023 - Amendment CXXXI. and article 13 of the Constitution of the Republika Srpska, *Official Gazette of the Republika Srpska*, no. 21/92, 28/94, 8/96, 13/96, 15/96, 16/96, 21/96, 21/02, 26/02, 30/02, 31/02, 69/02, 31/03, 98/03, 115/05, 117/05.

⁷ *Costello-Roberts v. The United Kingdom*, European Court of Human Rights, Application no. 13134/87, judgment of 25. 3. 1993, para. 36.

⁸ Opservatorij ljudskih prava: Bosna i Hercegovina. 2012. Pravo na zaštitu privatnog života. Available at: <https://opservatorij.wordpress.com/pravo-na-zastitu-privatnog-zivota-08/> (26. 5. 2025).

The ECtHR, when it comes to the protection of legal certainty, mostly relies on the provisions of Article 6 of the ECHR. This article regulates the rights of persons in criminal and civil proceedings, whereby paragraph 1 states that *"every person has the right to a fair, public trial before an independent and impartial court established by law, which will examine his case within a reasonable time, either in connection with the determination of civil rights and obligations, or in the case of an indictment for a criminal offense"*. ECtHR focuses on safeguarding human rights by addressing significant violations of the ECHR, particularly when national courts act contrary to its provisions. It promotes fair trials, consistent judicial practices, and legally grounded decisions to ensure legal certainty and protect individuals from arbitrary or unduly prolonged court procedures.

In relation to the topic of this paper, the ECtHR in the case of *Ringwald v. Croatia*⁹ made interesting observations on its role in protecting individuals' rights under the Convention. The Court stated that its function is not to correct errors of fact or law allegedly made by national courts, except insofar as those errors lead to a violation of the protected rights and freedoms. ECtHR rejects the role of a "court of fourth instance" and will not review national court judgments under Article 6(1) of the Convention unless their conclusions are manifestly arbitrary and unreasonable, emphasizing that Article 6(1) guarantees a fair trial but does not regulate evidence admissibility or assessment, which is governed by national laws. The majority of ECtHR applications involve claims of unlawful evidence obtained through special investigative measures, alleging violations of Articles 6 and 8.

The right to a fair trial is the right most frequently invoked by applicants to the Court. In view of the above, it is not surprising that there is a very rich case-law on the application of this article.¹⁰ The general elements of the concept of a fair trial that are common to the parties in all judicial proceedings are: a) the principle of adversarial proceedings, i.e. the right of the parties to be present at the proceedings and to be heard before the decision is taken, b) the principle of equality of arms and c) the right to a reasoned decision. Some add to the above elements, d) the prohibition on the use of unlawful evidence, although the Court has not yet expressed the aforementioned prohibition as a separate general element of the concept of a "fair trial" (Mrčela, Tripalo, & Valković, 2016, pp. 29-30). Due to the different legal definitions and rules by which states regulate the institution of illegal evidence, the ECtHR cannot establish uniform standards applicable to all legal systems of the member states, as this would lead to imposing certain rules on national legislation.

4. BALANCE BETWEEN THE EFFICIENCY OF CRIMINAL JUSTICE AND THE PROTECTION OF HUMAN RIGHTS

The efficiency of criminal proceedings is influenced by many factors, and in the literature, authors who have dealt with this in this region have observed this in the context of Article 6 of the ECHR and trial within a reasonable time, i.e. the short duration of the

⁹ *Ringwald v. Croatia*, European Court of Human Rights, Application no. 14590/15, the judgment of 22. 1. 2019.

¹⁰ Interights. 2010. *Article 6 of the European Convention on Human Rights - the right to a fair trial*, Handbook for Lawyers, INTERIGHTS. p. 2.

proceedings, most often in light of the defendant's right to a trial within a reasonable time. However, this should also be observed in relation to other subjects, because the efficient completion of criminal proceedings is in their interest, as well as the interest of society as a whole. The protection of the rights of the subjects of the proceedings and the efficiency of the criminal proceedings are in conflict. One cannot speak of an efficient criminal procedure if the rights of the defendant and other participants in the proceedings have been violated. Perhaps the best explanation of this relationship is from the period of the former Yugoslavia, when Cvijović (1985, p. 70) stated that the efficiency of criminal proceedings should be understood as a measure of the speed of proceedings, which ensures full respect for the lawfulness of the conduct of criminal proceedings and adjudication, and contributes to reducing the time from the moment of committing the criminal offence to the final adjudication to a realistic framework.

An efficient criminal justice system is vital for the common good, but it must prioritize human rights to ensure fair trials, balancing efficiency with fundamental freedoms to maintain confidence in justice and uphold the rule of law. Among other things, in the case of *Bykov v. Russia*¹¹, the ECtHR introduced a specific test to assess whether the proceedings as a whole were fair.

The test involves answers to these questions:

1. What is the alleged illegality of the evidence, and was any ECHR right, particularly Article 8, violated?
2. Could the applicant challenge the obtained evidence?
3. How significant was this evidence in the proceedings? Was it decisive for the outcome, and was there other supporting evidence?

The Court has already held that “*the general principles of fairness enshrined in Article 6 apply to all criminal proceedings, whatever the nature of the offence in question. Concern for the public interest cannot justify measures which nullify the very essence of the applicant’s rights of defence... as guaranteed by Article 6 of the Convention.*”¹²

When it comes to special investigative measures, which primarily include secret surveillance of communications and the use of undercover investigators in the case of *Ramanauskas v. Lithuania*¹³ before the ECtHR, the Court acknowledged the difficulties faced by the police in seeking and collecting evidence for detecting and investigating criminal offences. In order to carry out this task, the police increasingly have to use undercover investigators, informants, and secret investigative techniques, particularly in the fight against organised crime and corruption.¹⁴ Accordingly, the use of special investigative methods, in particular undercover techniques, does not in itself constitute a violation of

¹¹ *Bykov v. Russia*, European Court of Human Rights, Application no. 4378/02, judgment of 10. 3. 2009.

¹² *Bykov v. Russia*, European Court of Human Rights, Application no. 4378/02, judgment of 10. 3. 2009, para. 93.

¹³ *Ramanauskas v. Lithuania*, European Court of Human Rights, Application no. 74420/01, judgment of 5. 2. 2008.

¹⁴ *Ramanauskas v. Lithuania*, European Court of Human Rights, Application no. 74420/01, judgment of 5. 2. 2008, para. 49.

the right to a fair trial. However, because of the risk of police incitement that such techniques entail, they must be used within clearly defined limits in order to avoid a violation of the right to a fair trial.¹⁵

In its case law, the ECtHR has developed several criteria for protecting secret surveillance of communications, which must be prescribed by law in order to prevent abuses¹⁶. In this regard, the ECtHR examines whether the domestic legal solution clearly defines (Bećirović, 2024, p. 81):

1. The nature and type of criminal offenses for which a search warrant may be issued;
2. Category of persons whose communication can be intercepted;
3. Limitation of the duration of the interception;
4. Procedure for collection, use, and storage of collected data;
5. Precautions when transferring data to other parties;
6. Circumstances in which the obtained data can, or must, be deleted or destroyed.

If evidence is collected as part of a targeted interception of communications for national security reasons, the same six minimum requirements apply, but two more are added:

1. Plans for monitoring the implementation of secret surveillance measures;
2. Mechanisms for notification of intercepted communications and their content, as well as legal remedies provided for by national law.

In the case *A.L. AND E.J. v. France (dec.)* British applicants who failed to avail themselves of a domestic remedy in France, which could have effectively challenged the transfer of data under the European Investigation Order (EIO) issued by the United Kingdom and against the data discovery measure, the appeal was dismissed as inadmissible.¹⁷ The decision of the ECtHR on the request of the British A.L. and E.J. against France - 44715/20 and 47930/21 was made on September 24, 2024, and it is related to the decrypted communication application "EncroChat", which also applies to all other decrypted communications, including the "SKY ECC" application. The decision confirmed that the legality of the procedure by which France obtained the evidence cannot be questioned. The court emphasised that this aligns with the practice of the Court of the EU, which holds that the principle of mutual recognition prevents authorities from reassessing the legality of how another Member State collected evidence under an EIO. For the first time, the ECtHR also addressed, though not substantively, whether exchanging evidence obtained through special investigative actions complies with the law.

¹⁵ *Ramanuskas v. Lithuania*, European Court of Human Rights, Application no. 74420/01, judgment of 5. 2. 2008, para. 51.

¹⁶ *Huvig v France*, European Court of Human Rights, Application no. 11105/84, judgment of 24. 4. 1990; *Kruslin v. France*, European Court of Human Rights, Application no. 11801/85, judgment of 24. 4. 1990; *Valenzuela Contreras v. Spain*, European Court of Human Rights, application no. 27671/95, judgment of 30. 7. 1998; *Weber & Saravia v. Germany*, European Court of Human Rights, application no. 54934/00, decision on admissibility of 29. 6. 2006.; *Association for European Integration and Human Rights & Ekimdzhiev*, European Court of Human Rights, Application no. 62540/00, judgment of 28. 6. 2007. *Big Brother Watch v. the United Kingdom (GC)*, European Court of Human Rights, judgment of 25. 5. 2021.

¹⁷ *A. L. AND E.J. v. France (dec.)*, European Court of Human Rights, Application no. 44715/20 and 47930/21, judgement of 24. 9. 2024.

5. RIGHT TO DEFENSE AND USE OF DIGITAL EVIDENCE

Digital evidence represents a new concept of evidence, which has become ubiquitous in criminal proceedings, as there is no area of crime without a digital dimension (Casey, 2011, p. 3). Few studies have been done on how constitutional protections shape the admissibility of digital evidence, affecting the speed and outcome of criminal judgments. In one of the few (Novak, 2019), it turned out that overall, digital evidence does not seem to play a large role in federal criminal appeals filed within the U.S. Courts of Appeals (only 147 of the 45,030 federal, criminal cases affirmed or reversed for the years 2010 through in 2015). Digital evidence (e.g., from smartphones, social media, or IoT devices) can accelerate investigations by providing detailed data, but constitutional protections require warrants or specific legal conditions for searches, which can slow down evidence collection.¹⁸

There are different approaches in Bosnia and Herzegovina when it comes to handling digital evidence, and they are mainly based on the unequal views of judicial functionaries on this type of evidence, especially prosecutors, bearing in mind that in the legal system of BiH, the competence for conducting investigative proceedings is fully entrusted to them (Kavazović *et al.*, 2019, p. 353). The prosecutor manages, conducts, and supervises the investigation (see more: Simović, 2014; Lakić, 2014). This practically means his active and continuous engagement in planning and conducting the activities of authorised officials, i.e., selecting investigative actions for collecting digital evidence, but also supervising their efficiency and legality¹⁹. In addition to the prosecutor, so-called experts also play a significant role in handling digital evidence. Namely, the evidentiary action of searching computer systems, devices for storing computer and electronic data, mobile phones, and other similar devices according to criminal procedure provisions can only be undertaken with the help of these persons²⁰. The term "expert" is not defined in the criminal procedure codes, although it is used in several provisions contained in Articles: 34 (1) and (3), 51 (3), 86 (4) and (6), 94 (1), 185 (2), 187 (1), 355 (3), 356 (2), 373 (2) of the CPC of BiH. Sijerčić-Čolić defines an expert as a person of a certain profession who is called by the criminal procedure authority to clarify certain technical or other expert questions that arise in connection with the evidence obtained, or when questioning the suspect or accused or when undertaking other investigative actions (Sijerčić-Čolić, 2008, p. 431).

¹⁸ Delgado, A. The Impact of Digital Evidence in Today's Criminal Cases. Aaron & Delgado Associates. Available at: <https://www.communitylawfirm.com/blog/impact-digital-evidence-todays-criminal-cases> (26. 5. 2025).

¹⁹ Art. 35. (2) (a) of the Criminal Procedure Code of Bosnia and Herzegovina, *Official Gazette of Bosnia and Herzegovina*, no. 3/03, 32/03, 36/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 12/09, 16/09, 93/09, 72/13, 65/18.

²⁰ Art. 51(3) of the Criminal Procedure Code of Bosnia and Herzegovina. The same provision is contained in other procedural laws: Art. 65. (3) of the Criminal Procedure Code of the Federation of Bosnia and Herzegovina, *Official Gazette of the Federation of Bosnia and Herzegovina*, no. 35/03, 37/03, 56/03, 78/04, 28/05, 55/06, 27/07, 53/07, 9/09, 12/10, 8/13, 59/14. (hereinafter: CPC FBiH); Art. 115 (3) of the Criminal Procedure Code of the Republika Srpska ("Official Gazette of the RS", 53/2012, 91/2017 and 66/2018) (hereinafter referred to as: CPC RS); Art. 51 (3) of the Criminal Procedure Code of the Brčko District of Bosnia and Herzegovina, *Official Gazette of the Brčko District of Bosnia and Herzegovina*, no. 34/2013 - consolidated text and 27/2014 (hereinafter referred to as: CPC BD BiH).

6. LENGTH OF THE PROCEDURE AND THE ECTHR

The ECtHR recognised the complexity of the computer software that was created and allegedly used for the company's fraudulent accounting and tax evasion as a factor in the time it took for the tax inspectorate to assess whether its accounting records were in order and, if not, how much tax could have been avoided. However, this was not considered sufficient to justify the inspectorate taking almost twenty months to reach a conclusion on the matter, and this delay contributed to the finding in *Gančo v. Lithuania*²¹ that the criminal proceedings had been unreasonably prolonged, contrary to Article 6 § 1. In light of the right to a fair trial, challenges like maintaining a chain of custody, ensuring data integrity, and respecting privacy rights can complicate digital investigations, potentially delaying cases if evidence is deemed inadmissible due to constitutional violations (Stoykova, 2023).

7. PRACTICE OF CONSTITUTIONAL AND CRIMINAL LAW IN BOSNIA AND HERZEGOVINA

By reviewing the practice of the Constitutional Court of Bosnia and Herzegovina, we found that it was not established that the criminal proceedings lasted an unreasonably long time due to procedural errors in the collection of digital evidence. It is encouraging that there are few cases like the one we will shortly present, but because of the system of legal remedies here it could happen that the procedure lasts longer, that the first-instance decision was convicting and the second-instance was acquittal (the Supreme Court of the Federation of Bosnia and Herzegovina would still decide), and also that the decision was revoked (note that, unlike the Republic of Srpska, a case in the Federation of Bosnia and Herzegovina can only be revoked once or twice, the second-instance court has to decide on its own, the exception is the situation when the case goes to the Supreme Court). As a case study, we can cite a new example from practice in the Federation of Bosnia and Herzegovina. Namely, in a case that was first instanced before the Municipal Court of Tuzla, and based on the indictment of the Cantonal Prosecutor's Office of Tuzla,²² a verdict was reached in which the accused was acquitted of liability upon appeal by the Cantonal court of Goražde²³ (the Supreme Court of the Federation of Bosnia and Herzegovina delegated the case to this court), because of major failures by the prosecutor's office in Tuzla. For example, the prosecutor's office collected digital evidence originating from computer systems and mobile devices in such a way that the injured party photographed them and submitted them to the prosecutor's office as evidence. The Municipal and Cantonal Courts correctly concluded that the collection of evidence from the aforementioned systems can only be carried out by searching them, which is carried out by order of the court, whereby a copy of the documents located on the searched computer system or mobile device is made, and which is secured by entering a hash value for the purpose of later verification of authenticity, thus ensuring such data for further secure expert examination. The fact that the prosecution did not conduct a search of the computer

²¹ *Gančo v. Lithuania*, Application no. 42168/19, the judgment of 13. 7. 2021.

²² According to information from the CIN website, the acting prosecutor was sanctioned twice, and the second time he was given a public written warning for abuse of the TCMS.

²³ Judgment of the Cantonal court of Goražde, no. 32 0 K 427600 24 Kž 2 of 3. 7. 2024.

systems, or telephones, on which the injured party received the aforementioned messages, indicates that the evidence submitted in printed form, which was created electronically, was not collected in a lawful manner and could not be used in these proceedings nor could a court decision be based on them.

8. CONCLUSION

Judge Tim Eicke of the ECtHR points out that Article 6 of the ECHR guarantees the right to a fair trial, but does not lay down rules on the admissibility of evidence or its assessment. The Court has clearly adopted the position that, as long as the trial of an individual as a whole is “fair”, the admissibility of evidence and its assessment are matters that should primarily be dealt with by national law and national courts. The Constitution of BiH does not contain specific provisions relating to digital evidence, but general rules relating to human rights and freedoms, including the protection of privacy and freedom of communication, may affect how digital evidence is used. Article 8 of the ECHR, which is integrated into the legal system of BiH, guarantees the right to privacy, which may be relevant when considering the legality of the collection and use of digital evidence. For digital evidence to be admissible in court, there must be validation of the source of the evidence, the accuracy of the data, and a way to protect it from unauthorised changes. Digital evidence, such as emails, videos, computer or mobile device recordings, must be properly verified, and the process of collecting and storing data must be transparent to ensure its validity in court.

In Bosnia and Herzegovina, there are indications and examples suggesting that improper or controversial collection of digital evidence can affect the length of judicial proceedings, especially in cases of organised crime and corruption. Based on the available information, we can conclude that certain controversies related to digital evidence still exist. In the last few years, there have been investigations in Bosnia and Herzegovina that used digital evidence, such as encrypted messages from applications such as Sky and Anom. According to reports, this evidence was often collected through international cooperation with foreign law enforcement agencies, raising questions about the legality and procedures of the collection. At the annual conference of the Judicial Forum for BiH in 2022, it was emphasised that the courts must decide whether such evidence is admissible and whether there has been a violation of the suspects' human rights. In some cases, the public and the media expressed dissatisfaction with the slow reactions of the BiH Prosecutor's Office to publish digital evidence, such as the Sky correspondence. This shows that the perception of improper or slow collection of evidence can further complicate and prolong proceedings, as public pressure and political interests often intertwine with judicial processes. In conclusion, although there is no direct and universal established conclusion that the improper collection of digital evidence in all cases in BiH caused lengthy procedures, and especially not that the duration of the procedure due to digital evidence was unreasonably long considering the parameters of the Constitutional Court of BiH and the ECtHR, there are concrete examples and legal frameworks that show that such situations can significantly slow down the process. Long duration may arise because of necessary legality checks, appeals by parties, or even international cooperation that requires additional time.

LIST OF REFERENCES

- Bećirović, A. 2024. Navigating the digital labyrinth: challenges facing the judiciary in "handling" digital evidence. *Legal Chronicles*, 17(9), pp. 77-82.
- Cvijović, O. 1985. The influence of mutual relations between the main procedural subjects on the efficiency of criminal proceedings. *Yugoslav Review of Criminology and Criminal Law*, 4, pp. 69-79.
- Delgado, A. The Impact of Digital Evidence in Today's Criminal Cases. Aaron & Delgado Associates. Available at: <https://www.communitylawfirm.com/blog/impact-digital-evidence-todays-criminal-cases> (26. 5. 2025).
- Adžajlić Hodžić, M. et al. 2021. *Special investigative measures in the practice of courts in Bosnia and Herzegovina*. Sarajevo: Geneva Centre for Security Sector Governance (DCAF).
- Casey, E. 2011. *Digital Evidence and Computer Crime - Forensic Science, Computers, and the Internet*. Waltham, San Diego, London: Elsevier Academic Press.
- Kavazović, M. et al. 2019. Forensic Processing with Digital Evidence in the Practice of Police Agencies in Bosnia and Herzegovina. *Criminal Topics*, 19(5), pp. 351-388.
- Knežević, Z. & Dumanjić E. 2019. *Special investigative actions*. Sarajevo: The AIRE Centre.
- Lakić, L. 2014. Experiences and Perceived Problems in the Application of Prosecutorial Investigation in BiH. In: I. Jovanović & A. Petrović-Jovanović (eds.), *Prosecutorial Investigation: Regional Criminal Procedure Legislation and Experiences in Application*. Belgrade: OSCE Mission to Serbia, pp. 89-106.
- Mrčela M., Tripalo D. & Valković L. 2016. *Handbook for participants, Selected chapters of the European Convention on Human Rights and Fundamental Freedoms – criminal law aspect*. Zagreb: Judicial Academy.
- Novak, M. 2019. Digital Evidence in Criminal Cases Before the U.S. Courts of Appeal: Trends and Issues for Consideration. *Journal of Digital Forensics, Security and Law*, 14(3), pp. 1-42. <https://doi.org/10.15394/jdfsl.2019.1609>
- Opservatorij ljudskih prava: Bosna i Hercegovina. 2012. Pravo na zaštitu privatnog života. Available at: <https://opservatorij.wordpress.com/pravo-na-zastitu-privatnog-zivota-08/> (26. 5. 2025).
- Sijerčić-Čolić, H. 2008. *Krivično procesno pravo. Knj. 1, Krivičnoprocesni subjekti i krivičnoprocesne radnje*. Sarajevo: Faculty of Law, University of Sarajevo.
- Simović, M. N. 2014. The Concept of Prosecutorial Investigation in the Criminal Procedure Code of Bosnia and Herzegovina: Status and Problems. pp. 43-58. In: I. Jovanović & A. Petrović-Jovanović (eds.), *Prosecutorial Investigation: Regional Criminal Procedure Legislation and Experiences in Application*. Belgrade: OSCE Mission to Serbia, pp. 43-58.
- Stoykova, R. 2023. The right to a fair trial as a conceptual framework for digital evidence rules in criminal investigations, *Computer Law & Security Review*, 49, pp. 1-26. <https://doi.org/10.1016/j.clsr.2023.105801>

Legal Sources and case law

- A. L. ANDE. J. v. France* (dec.), European Court of Human Rights, Application no. 44715/20 and 47930/21, judgment of 24. 9. 2024.
- Association for European Integration and Human Rights & Ekimdzhiiev*, European Court of Human Rights, Application no. 62540/00, judgment of 28. 6. 2007.
- Big Brother Watch v. the United Kingdom (GC)*, European Court of Human Rights, judgment of 25. 5. 2021.
- Bykov v. Russia*, European Court of Human Rights, Application no. 4378/02, judgment of 10. 3. 2009.
- Council of Europe. 1950. European Convention on Human Rights and Fundamental Freedoms.
- Constitution of Bosnia and Herzegovina, Aneks IV Opšteg okvirnog sporazuma za mir u Bosni i Hercegovini and *Official Gazette of Bosnia and Herzegovina*, no. 25/2009 – Amendment I.
- Constitution of the Federation of Bosnia and Herzegovina, *Official Gazette of the Federation of Bosnia and Herzegovina*, no. 1/1994, 1/1994 - Amendment I, 13/1997 - Amendments II-XXIV, 13/1997 - Amendments XXV and XXVI, 16/2002 - Amendments XXVII-LIV, 22/2002 - Amendments LVI-LXIII, 52/2002 - Amendments LXIV-LXXXVII, 60/2002 – correction of the Amendment LXXXI, 18/2003 - Amendment LXXXVIII, 63/2003 - Amendments LXXXIX-XCIV, 9/2004 - Amandmani XCV-CII, 32/2007 - correction 20/2004 - Amendments CIII and CIV, 33/2004 - Amendment CV, 71/2005 - Amendments CVI-CVIII, 72/2005 - Amendment CVI, 88/2008 - Amendment CIX, 79/2022 - Amendments CX-CXXX, 80/2022 – correction and 31/2023 - Amendment CXXXI.
- Constitution of the Republika Srpska, *Official Gazette of the Republika Srpska*, no. 21/92, 28/94, 8/96, 13/96, 15/96, 16/96, 21/96, 21/02, 26/02, 30/02, 31/02, 69/02, 31/03, 98/03, 115/05, 117/05.
- Criminal Procedure Code of Bosnia and Herzegovina, *Official Gazette of Bosnia and Herzegovina*, no. 3/03, 32/03, 36/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 12/09, 16/09, 93/09, 72/13, 65/18.
- Criminal Procedure Code of the Brčko District of Bosnia and Herzegovina, *Official Gazette of the Brčko District of Bosnia and Herzegovina*, no. 34/2013 - consolidated text and 27/2014.
- Criminal Procedure Code of the Federation of Bosnia and Herzegovina, *Official Gazette of the Federation of Bosnia and Herzegovina*, no. 35/03, 37/03, 56/03, 78/04, 28/05, 55/06, 27/07, 53/07, 9/09, 12/10, 8/13, 59/14.
- Criminal Procedure Code of the Republika Srpska, *Official Gazette of the Republika Srpska*, no. 53/2012, 91/2017 and 66/2018.
- Huvig v France*, European Court of Human Rights, Application no. 11105/84, judgment of 24. 4. 1990.
- Gančo v. Lithuania*, Application no. 42168/19, the judgment of 13. 7. 2021.
- Kruslin v. France*, European Court of Human Rights, Application no. 11801/85, judgment of 24. 4. 1990.

Judgment of the Cantonal court of Goražde, no. 32 0 K 427600 24 Kž 2 of 3. 7. 2024.

Ramanuskas v. Lithuania, European Court of Human Rights, Application no. 74420/01, judgment of 5. 2. 2008.

Szabó and Vissy v. Hungary, European Court of Human Rights, Application no. 37138/14, Judgment of 12. 1. 2006.

Dragojević v. Republic of Croatia, European Court of Human Rights, Application no. 68955/11, Judgment of 15. 1. 2015.

Costello-Roberts v. The United Kingdom, European Court of Human Rights, Application no. 13134/87, judgment of 25. 3. 1993.

Ringwald v. Croatia, European Court of Human Rights, Application no. 14590/15, the judgment of 22. 1. 2019.

Valenzuela Contreras v. Spain, European Court of Human Rights, application no. 27671/95, judgment of 30. 7. 1998.

Weber & Saravia v. Germany, European Court of Human Rights, application no. 54934/00, decision on admissibility of 29. 6. 2006.

