USE OF DIGITAL EVIDENCE IN CRIMINAL PROCESS: SOME ISSUES OF RIGHT TO PRIVACY PROTECTION

Prysiazhniuk Ivan

DOI: https://doi.org/10.61345/1339-7915.2023.5.11

Annotation. The rapid development of digital technologies makes life easier in many ways. One of these advantages is the ability to use digital evidence in criminal proceedings. At the same time, this gives rise to new challenges in protecting the right to privacy, since digital evidence often contains a large amount of personal information. Thus, the author of the article aims at exploring the issues of balance between the use of digital evidence in criminal justice and the protection of the right to privacy.

The research methodology includes an analysis of scientific publications, current legal provisions, case law, and international standards. The author of the article emphasizes that, on the one hand, the legislation operates with the concept of "digital evidence" and emphasizes the possibility of its use. On the other hand, the norms of international law and Ukrainian legislation determine the need to respect the right of every person to privacy. This raises the issue of combining these two phenomena.

An analysis of the ECtHR case law has shown that this issue is important. The Court does not consider digital evidence, the acquisition of which has led to a violation of the right to privacy, to be legitimate. Based on the analysis of the case law, the author emphasizes the critical importance of the right to privacy as a basic human right that should be upheld even during a criminal investigation.

The results indicate the need for clear legislative regulation of the use of digital evidence, ensuring its proportionality, and the need to take into account the right to privacy as a fundamental right. The conclusions of the article emphasize the importance of international standards and case law in shaping approaches to the use of digital evidence, with a particular focus on the protection of the right to privacy in the context of criminal justice. The author also proposes a number of approaches that can ensure the lawful and appropriate use of digital evidence.

Key words: digital evidence, right to privacy, criminal proceedings, criminal process, evidence in criminal proceedings, human rights.

1. Introduction.

In today's world, digital technology has penetrated every aspect of our lives. Therefore, digital evidence is becoming increasingly important in criminal justice. From cell phones to computer networks, digital traces left by humans can play a key role in crime investigations and trials. Digital evidence not only helps to recreate events and establish facts that would be inaccessible or invisible to traditional investigative methods, but also contributes to the maintenance of a fair trial. All in all, their benefits are quite obvious.

In addition, the need to use digital evidence is also driven by the latest forms of crime. Modern cybercrime, with its unique and unconventional methods of committing crimes, is becoming increasingly widespread. This makes it important to study the correct legal regulation of the use

of electronic evidence in criminal proceedings. This issue becomes even more important given that a significant number of modern crimes are committed with the help of the latest information technologies. Digital evidence, which is increasingly used in criminal proceedings, is becoming a key part of the evidence base, emphasizing the need for adequate legislative regulation of its use in Ukraine [6, p. 159].

Along with the clear advantage of digital evidence, we also face a challenge. It will be manifested in the issue of the need to properly ensure the right to privacy of the individual. That is, to ensure that the collection and use of this data is done in a manner that respects the right to privacy of each individual. Finding the right balance is important. This is necessary to ensure that the full potential of digital evidence is utilized on the one hand. On the other hand, it will ensure that human rights are respected. The right to privacy is a fundamental human right. Excessive interference with privacy through uncontrolled collection of digital data may violate this right. Thus, a balance needs to be struck to ensure that the collection and use of digital evidence does not violate personal rights and freedoms.

To ensure the legitimacy and legitimacy of criminal justice, it is imperative that the process of collecting and analyzing digital evidence is carried out in strict accordance with established legal norms and procedures. This implies the implementation of adequate legal mechanisms to prevent arbitrary and unlawful data collection.

In the context of the rapid development of technologies that offer new opportunities for information extraction and analysis, the legislative framework and judicial practice must adapt to these changes to avoid violations of privacy rights in the collection of such data. In the face of these transformations, it is crucial to establish and maintain an optimal balance between the needs of effective investigation and the protection of individual rights and freedoms, which is the foundation of a fair and effective criminal justice system.

2. Analysis of scientific publications.

The relevant issue has been raised in Ukrainian academic circles in the works of various scholars. The author drew special attention to the scientific contribution of Dehtiarova O. The researcher notes that the procedure of proof is fundamental. In this process, the key is the work of the investigator, who is responsible for verifying and evaluating the evidence collected, as well as for its adequacy to form an informed decision. This aspect becomes particularly challenging in the context of digital evidence, which, along with traditional paper documents, requires specialized approaches to its recording and evaluation as evidence. Therefore, special attention should be paid to the review and processing of such evidence in the context of its use in criminal justice [4].

In the context of the research topic, special attention should be paid to the work of domestic scholars Garasymiv O.I., Marko S.I., Ryashko O.V. They consider current issues that arise in the context of practical application of digital evidence in Ukraine. The authors note that today, the Ukrainian judicial system is characterized by some uncertainty in determining and assessing the reliability of information contained in digital documents. In addition, unfortunately, unified criteria have not yet been developed that would allow digital documents to fully fulfill the role of evidence in criminal proceedings. The constant growth in the use of innovative technologies has two sides of the coin, both positive and negative. The main problem in this legal institution is the lack of clear legislative regulation of the procedures for seizure, evaluation and analysis of electronic evidence at the level of procedural law. Their work seems particularly relevant, as they pay some attention to possible violations of the right to privacy. However, they provide only certain general recommendations [6].

Based on the analysis of academic sources, it can be concluded that there is an intense debate in the scientific community on the issue of digital evidence in criminal proceedings. A wide range of studies focuses on the adequacy and effectiveness of the implementation of this type of evidence in practice. A number of scientific works reviewed above emphasize the difficulties associated with the protection of the right to privacy in the context of the use of digital evidence. Nevertheless, despite the recognition of privacy as a key and inalienable human right, there is no holistic and

comprehensive approach to the protection of privacy in the context of digital evidence in the national scientific literature, which requires further elaboration of the theoretical foundations and development of practical recommendations to address this issue.

3. The aim of the work.

The aim of the article is to explore the issue of the balance between the use of digital evidence in criminal justice and the protection of the right to privacy. The article focuses on the analysis of current legal provisions, case law and international standards, as well as on identifying ways to address the problems associated with the collection and use of digital data, while ensuring the protection of fundamental human rights.

4. Review and discussion.

Digital evidence can be defined as information data that serves as a tool or means of implementing a criminal act, contains electronic and digital indicators of criminal activity, or is the subject or object of a criminal violation. This data acquires its significance and relevance in the context of legal consideration of criminal cases, acting as a key element in the process of establishing facts and evidence [4, p. 276].

In 2017, Ukrainian legislation underwent significant changes aimed at improving the process of proof. At this time, the definition of evidence in the country's procedural codes was expanded, including, in particular, the introduction of the concept of electronic evidence into legislative texts [13, p. 49]. Thus, according to Article 99 of the Criminal Procedure Code of Ukraine, 2012, digital files, such as photographic, sound recording, video recording and other media, including computer data, are qualified as "documents". And documents, in turn, are considered material evidence if they meet the requirements established by law [9]. In addition, the Code allows for certain cases of recording certain investigative search actions in digital form. However, despite the fact that this concept has been introduced into legislative practice, there are still significant gaps in the work of this institution that affect the ability of persons to present electronic evidence in court.

There are also a number of problems associated with their use. One of the main problems is to ensure the authentication of digital evidence – confirmation that the data has not been altered. This requires sophisticated technical means and techniques [12, p. 209]. Digital data is easier to change and manipulate than physical evidence. Therefore, there is a risk that the evidence may be falsified or tampered with.

The problem also manifests itself in technical and competence issues. Investigations involving digital evidence require specialized technical knowledge and resources that are not always available to law enforcement agencies. The rapid development of technology can lead to the rapid obsolescence of software and hardware used to collect and analyze digital evidence.

In cases of transnational crimes, the collection and processing of digital evidence may require international cooperation and collaboration, which can be complicated by differences in legislation. In many jurisdictions, legislation on digital evidence is still evolving, which can lead to legal uncertainty. Thus, in Ukrainian legal practice, there are a significant number of cases where applications are left without consideration due to the failure of the submitted evidence to meet the established criteria. Particular difficulties arise from the unclear understanding of the difference between written evidence and electronic evidence in the form of paper copies. As a potential way forward for the criminal justice system, it may be promising to grant electronic evidence an independent status, which may facilitate its more effective use in court proceedings [6, p. 162].

One of the most pressing problems in the analysis of electronic data storage devices in criminal proceedings is the virtually unlimited access to confidential information by the prosecution. This poses a threat of violation of privacy rights. Therefore, there is a requirement to clearly define at the legislative level the parameters and criteria under which the use of such electronic data in criminal

investigations may be considered inadmissible in order to ensure a balance between the needs of the investigation and the protection of personal rights and freedoms. This issue is at the center of discussions on the digitalization of criminal proceedings. And this is not unexpected, since the right to privacy is an inalienable human right and the use of digital evidence may violate it.

Ukrainian legislation contains rules on the use of digital evidence, while ensuring the right to privacy of each individual. According to Article 32 of the Constitution of Ukraine, 1996 no one shall be subjected to interference with his or her private and family life, except in cases provided for by the Constitution of Ukraine [8].

International law also warns about the need to ensure the right to privacy. A large number of such norms have been adopted, so we will consider only some of the most important ones in the context of the topic of the article. Thus, according to Article 12 of the Universal Declaration of Human Rights, 1948, the right of everyone to protection from arbitrary interference with his or her private and family life is recognized [14]. The norms of this document are declarative, but they were further embodied in the International Covenant on Civil and Political Rights, 1966. According to Article 7 of this Covenant, no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence [7].

It is also worth noting two important legal acts adopted by the Council of Europe. The first is the European Convention on Human Rights, 1950. Article 8 of the Convention guarantees the right to respect for private and family life, home and correspondence [5]. The second is the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981. This document is the first international treaty aimed at protecting the right to privacy in the context of automated processing of personal data [3]. Both documents have been ratified by Ukraine, and thus are also part of its national legislation.

The General Data Protection Regulation (GDPR), 2016 deserves important attention. Although the document focuses primarily on regulating the processing of personal data for commercial purposes, it also has important implications for the use of digital evidence in criminal cases. The GDPR sets strict rules for the processing of personal data. This includes the collection, storage, transfer and use of any information that can identify a person. In the context of criminal law, this means that law enforcement agencies and courts must follow these rules when collecting and using digital evidence.

The GDPR emphasizes the right to privacy. This affects how digital data can be collected in criminal investigations. For example, bulk data collection without proper justification or consent may be considered a violation of the GDPR. The document also requires that data processing be limited to the necessary minimum and used only for specified, explicit and legitimate purposes. This means that law enforcement agencies must precisely justify the need to collect specific data for a criminal investigation.

At the same time, the GDPR recognizes that the processing of personal data may be necessary for the performance of law enforcement tasks [11]. Thus, there are certain exemptions for law enforcement agencies, but these exemptions still require compliance with the basic data protection principles.

The aforementioned norms and standards contribute to the formation of the international legal framework for the protection of the right to privacy, establishing the obligation of states to ensure adequate protection of personal data of citizens. To summarize the provisions of international legal acts on the protection of the human right to privacy, it can be noted that these norms provide protection against arbitrary or unlawful interference with privacy, which is critical when collecting digital evidence, which often contains confidential information. In addition, the norms laid down in international treaties require that the collection and use of digital data be carried out legitimately, i.e. with sufficient legal grounds and subject to clear criteria and restrictions.

International standards emphasize the principles of proportionality and necessity, according to which any interference with the right to privacy must be justified by a specific need for a fair investigation and must be proportionate to the measures taken. All these aspects should be taken into account in the development and implementation of national legislation and practices related to digital evidence to ensure a fair balance between effective investigation and the protection of privacy rights.

For a deeper understanding of the problem, let us consider the case law of the ECtHR. In particular, we will consider cases on violation of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms, 1950 [5]. Thus, we note the Case of Benedik v. Slovenia under application 62357/14, 2018. The judgment of the European Court of Human Rights found a violation of the plaintiff's right to respect for private life. Benedik was convicted of distributing child pornography based on evidence that he claimed was obtained illegally due to the lack of proper court authorization to access the relevant information.

The case concerned a situation where Slovenian law enforcement authorities did not obtain a court order to access subscriber data associated with a dynamic IP address used in a file-sharing network. The applicant, Igor Benedik, was identified after exchanging files in this network, which raises the question of the legality of data collection and use in criminal proceedings.

The European Court of Human Rights found that the provisions of the Law on Criminal Procedure applied by the Slovenian police, which allow the police to request information from electronic communication operators about users of certain means of communication whose personal data are not in accessible registers, did not meet the criteria of "conformity with the law" under the Convention. Analyzing this law, the court determined that it did not contain sufficient transparency, did not provide adequate protection against interference, did not have adequate safeguards against abuse, and did not provide for independent supervision of the actions of the police using these powers. The Court ruled that there had been a violation of Article 8 of the Convention, as the police had to obtain a court order [1].

Thus, the judgment in this case emphasizes the critical need to strike a proper balance between the effectiveness of law enforcement measures and the protection of privacy rights when using digital evidence. This decision emphasizes that the development and application of legal rules on digital evidence should take into account not only the needs of law enforcement agencies, but also the fundamental rights and freedoms of individuals. The judgment also suggests that the right to privacy is fundamental and cannot be violated in the process of collecting and using evidence in criminal justice. This right acts as an inviolable basis that must be taken into account and protected in all aspects of a criminal investigation. In the process of evidence in criminal justice, the right to privacy takes precedence over purely procedural aspects. This means that no measures may be taken that would unreasonably violate this right, even if such measures may facilitate the collection of evidence. Furthermore, any violation of the right to privacy during the course of evidence should be considered inadmissible and subject to proper legal challenge. No criminal proceedings can justify arbitrary interference with a person's privacy.

Among the most recent cases, it is worth highlighting the case of Glukhin v. Russia, application no. 11519/20, 2023. Although this case concerns an administrative offense rather than a criminal offense, we still consider it appropriate to consider it within the framework of this study. After all, the judgment in this case is quite new, and it can show the current attitude of the ECtHR to the issue of the right to respect for private life in the process of proof. Let us briefly consider the circumstances of the case. On August 23, 2019, the applicant was traveling in the Moscow metro with a life-size cardboard figure of political activist Konstantin Kotov, who was holding a banner with the inscription: "You must be kidding. I am Konstantin Kotov. I face up to five years in prison for peaceful protests." According to a police report of August 24, 2019, the department for combating extremism, while monitoring the Internet, found an image of the applicant with this poster at a metro station. The department then recorded screenshots from the Telegram channel, which contained images and videos of the applicant holding a cardboard figure of Mr. Kotov at the metro station and on the train. These images clearly showed the text on the poster. The department made printouts of these screenshots and stored them in accordance with the Code of Administrative Offenses.

Another report from the same day shows that the department received surveillance footage from the subway stations. On August 27, 2019, the department reviewed these recordings, created screenshots of the applicant's image, printed them out, and stored them in the case file. It is worth noting that in the spring of 2018, cameras with face recognition technology were installed at Moscow metro stations, and in 2019, their real-time testing began. The applicant was brought to administrative responsibility for violating the established procedure for holding mass events. He complained of a

violation of his right to freedom of expression (Article 10 of the Convention) and his right to privacy (Article 8 of the Convention) [5].

In his privacy complaint, the applicant claimed that his identity had been established and he had been detained using data obtained from a video surveillance system equipped with a face recognition function. He argued that the process of collecting, analyzing and archiving his personal data was carried out without proper legal authorization (e.g., without a court order) and that the legal framework authorizing such actions was too vague and did not meet the criteria of "quality of law".

Subsequently, the European Court of Human Rights applied a three-step test to analyze the legitimacy of this interference. The Court emphasized that national legislation should include a set of protective measures regarding the circulation of personal data, in particular in the context of their automated processing and use for law enforcement purposes.

In addition, the Court took into account the nature and seriousness of the alleged crime as a key aspect in its analysis. The European Court of Human Rights noted that the applicant was prosecuted for an administrative violation, which consists in organizing an unauthorized one-man demonstration. The absence of charges of committing harmful acts during the action, such as blocking traffic, damaging property or committing acts of violence, was also taken into account. The Court noted that the use of facial recognition technology to identify and detain participants in peaceful demonstrations can create an intimidating effect on their right to freedom of expression and assembly. As a result, the ECtHR found a violation of Article 8 of the Convention [2].

Therefore, the judgment of the European Court of Human Rights in this case has a significant impact on the protection of the right to privacy in the context of the collection and use of evidence. The judgment emphasizes the need to maintain high standards in the processing of personal data, especially when technologies such as face recognition are used. The judgment identifies the criteria of necessity and proportionality as fundamental in assessing any interference with the right to privacy. It emphasizes that the use of personal data must be justified and correspond to a real need. Moreover, the ECtHR confirms the importance of having a clear and precise legal basis for any type of personal data processing, especially in the context of law enforcement. Thus, this ECtHR judgment is an important step in strengthening the protection of the right to privacy in the context of evidence, emphasizing the need to strike a balance between law enforcement needs and fundamental rights and freedoms of individuals.

Based on the analyzed ECtHR case law, the following aspects of the use of digital evidence in criminal proceedings can be identified:

the need for clear legislative regulation of digital evidence collection procedures to prevent arbitrary and unlawful interference with the privacy of individuals;

the practice emphasizes the importance of the right to privacy as a fundamental human right that must be protected even in the context of a criminal investigation;

the need for independent oversight of the collection and use of digital evidence to prevent abuse and ensure transparency is substantiated;

the need for compliance of domestic legislation with international standards and agreements in the field of human rights protection is demonstrated.

Given the dynamic technological development, there is a significant probability that in the near future the national judicial system will completely switch to the electronic format of proof [10, p. 44]. Ensuring a balance between the effective use of digital evidence and the protection of the right to privacy requires a comprehensive approach which includes a number of the author's proposals. First of all, it is necessary to develop a clear legislative framework for the use of digital evidence. Unfortunately, neither the legislation nor the analyzed practice contains a clear framework that is admissible for the use of digital evidence. A detailed and specific legal framework regulating the collection, processing, storage and use of digital evidence should be established. This framework

should include clear criteria and procedures, as well as define the limits of permissible interference with privacy.

Proportionality and necessity should also be regulated. Thus, the use of digital evidence must be proportionate and justified in accordance with the seriousness of the criminal proceedings, in order to prevent excessive interference with privacy. Thus, when analyzing the case of Glukhin v Russia, the ECtHR, among other things, applied the criterion of "gravity of the case". In these circumstances, the applicant's guilt was not recognized as so high that it could justify interference with his private life. Therefore, the limits of possible interference should be clearly defined. For this purpose, it is advisable to develop "severity criteria" that will correlate with the possibility of using digital evidence in criminal proceedings.

In this context, it seems to us that there should be proper institutional support for relevant evidence, including the introduction of proper oversight. Establishing independent supervisory bodies to monitor compliance with the rules and procedures for the collection and use of digital evidence is critical to preventing abuse in this area. In this regard, it also seems important to organize specialized courses and trainings for law enforcement officers on the ethical aspects of using digital evidence and its impact on privacy. It is important to ensure close cooperation between law enforcement, IT professionals and lawyers to develop and apply best practices for collecting and processing digital evidence. In addition, the use of cryptographic methods to ensure the integrity and authenticity of digital evidence can prevent its manipulation or tampering.

5. Conclusions.

In summary, we can conclude that the use of digital evidence must be balanced with respect for the right to privacy. It is important to develop a clear legislative framework that defines the limits of the use of digital evidence. It is also necessary to guarantee the proportionality of measures and transparency of the data collection process. The role of international standards in protecting human rights is very important, including in the legal regulation of digital evidence. Analysis of court decisions and precedents is critical to understanding how modern justice adapts to technological changes and how these changes affect the protection of the right to privacy. Judicial practice, especially decisions of international courts, shapes approaches to the use of digital evidence, pointing to the need to regulate it and ensure the right to privacy, which is fundamental in modern legal proceedings.

It is important to address the balance between digital evidence and the right to privacy. This includes the establishment of clear legal rules governing the collection and processing of digital data, as well as the introduction of a system of independent oversight of their use. In addition, it is necessary to guarantee the proportionality of the use of digital materials, ensure the protection of personal data, and develop mechanisms to prevent abuse.

The prospect of further research is related to the constant technological development, which, in turn, raises new issues regarding the collection and use of digital evidence.

References:

1. Case of Benedik v. Slovenia (2018). Application no. 62357/14. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-182455%22]}.
2. Case of Glukhin v Russia (2023). Application no. 11519/20. URL: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-225655%22]}.
3. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981). URL: https://rm.coe.int/1680078b37.
4. Dehtiarova O. (2021). Dokazuvannia u kryminalnomu provadzhenni na pidstavi elektronnykh dokaziv [Evidence in criminal proceedings on the basis of electronic evidence]. Trybuna

molodoho vchenoho. Yurydychnyi visnyk – The Tribune of the Young Scientist. The Legal Bulletin, 6, 273–278 [in Ukrainian].

5. European Convention on Human Rights (1950). URL: https://www.echr.coe.int/documents/d/echr/convention_ENG.

6. Garasymiv O.I., Marko S.I., Ryashko O.V. (2023). Tsyfrovi dokazy: deiaki problemni pytannia shchodo yikh poniattia ta vykorystannia u kryminalnomu sudochynstvi. [Digital evidence: some problematic issues regarding its concept and use in criminal justice]. Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu – Scientific Bulletin of Uzhhorod National University, 75. 158–162 [in Ukrainian].

7. International Covenant on Civil and Political Rights (1966). General Assembly resolution 2200A (XXI). URL: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

8. Konstytutsiia Ukrainy (1996): Dokument № 254k/96-VR [Constitution of Ukraine: Document No. 254к/96-ВР]. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text [in Ukrainian].

9. Kryminalnyi protsesualnyi kodeks Ukraiiny (2012): Zakon Ukrainy № No. 4651-VI [Criminal Procedure Code of Ukraine (2012): Law of Ukraine No. 4651-VI]. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text [in Ukrainian].

10. Polunina O. O. (2020). Elektronni dokazy yak osoblyvyi zasib dokazuvannia u tsyvilnomu protsesi [Electronic evidence as a special means of proof in civil proceedings]. Reformuvannia tsyvilnoho protsesualnoho prava v umovakh intehratsiinykhprotsesiv v Ukraini – Reforming civil procedure law in the context of integration processes in Ukraine, 41–45.

11. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016). URL: https://www.eumonitor.eu/9353000/1/j4nvk6yhcbpeywk_j9vvik7m1c3gyxp/vk3t7p3lbczq.

12. Sirenko O. V. (2021). Сіренко О.В. Elektronni dokazy u kryminalnomu provadzhenni [Electronic Evidence in Criminal Proceedings]. Mizhnarodnyi yurydychnyi visnyk: aktualni problemy suchasnosti (teoriia ta praktyka) – International Legal Bulletin: topical issues of our time (theory and practice), 14, 208-214 [in Ukrainian].

13. Solonchuk I.V., Balinska V.O., Herashchenko Ya.V. (2021) Elektronni dokazy u tsyvilnomu sudochynstvi: perevahy ta nedoliky zakonodavchykh novovveden. [Electronic evidence in civil proceedings: advantages and disadvantages of legislative innovation]. Juris Europensis Scientia, 2, 48–52 [in Ukrainian].

14. Universal Declaration of Human Rights (1948). URL: https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf.

Ivan Prysiazhniuk,
Doctor of Law,
Associate Professor of the Department of Criminal Law, Process and Forensics?
Kyiv University of Intellectual Property and Law National University
Odessa Law Academy,
Kyiv, Ukraine