DIGITAL EVIDENCE IN CRIMINAL PROCEEDINGS: INTERNATIONAL STANDARDS AND CHALLENGES

Umarova Nazokat Fakhriddinovna
Student of Tashkent state university of Law
Criminal justice faculty
unazokat05@gmail.com
https://orcid.org/0009-0003-7151-8595
https://doi.org/10.5281/zenodo.20483941

Abstract: The rapid development of information technologies and digital communications has significantly transformed modern criminal proceedings. Digital evidence has become one of the most important elements in investigating cybercrime, financial crimes, terrorism, and transnational organized crime. This article examines the legal nature of digital evidence, analyzes international standards regulating its collection and admissibility, and identifies major challenges arising in criminal proceedings. Particular attention is devoted to issues of authenticity, reliability, jurisdiction, privacy protection, and international cooperation in obtaining electronic evidence. The article also evaluates the legal framework of the Republic of Uzbekistan concerning digital evidence and proposes recommendations aimed at harmonizing national legislation with international legal standards.

Keywords: digital evidence, criminal proceedings, cybercrime, electronic evidence, international law, Budapest Convention, criminal justice, cybersecurity, admissibility of evidence, electronic investigations.

Annotatsiya: Axborot texnologiyalari va raqamli kommunikatsiyalarning jadal rivojlanishi zamonaviy jinoyat protsessini tubdan o‘zgartirdi. Raqamli dalillar kiberjinoyatlar, moliyaviy jinoyatlar, terrorizm hamda transmilliy uyushgan jinoyatchilikni tergov qilishda eng muhim vositalardan biriga aylandi. Mazkur maqolada raqamli dalillarning huquqiy tabiati, ularni yig‘ish va sudda qo‘llashni tartibga soluvchi xalqaro standartlar hamda jinoyat protsessida yuzaga kelayotgan asosiy muammolar tahlil qilinadi. Shuningdek, autentiklik, ishonchlilik, yurisdiksiya, shaxsiy hayotni himoya qilish va elektron dalillarni olishdagi xalqaro hamkorlik masalalariga alohida e’tibor qaratilgan. Maqolada O‘zbekiston Respublikasining raqamli dalillar sohasidagi qonunchiligi ham o‘rganilib, milliy qonunchilikni xalqaro standartlarga uyg‘unlashtirish yuzasidan takliflar ishlab chiqiladi.

Kalit so‘zlar: raqamli dalillar, jinoyat protsessi, kiberjinoyatchilik, elektron dalillar, xalqaro huquq, Budapesht konvensiyasi, jinoiy odil sudlov, kiberxavfsizlik, dalillarning maqbulligi, elektron tergov.

Аннотация: Стремительное развитие информационных технологий и цифровых коммуникаций существенно трансформировало современное уголовное судопроизводство. Цифровые доказательства стали одним из важнейших элементов расследования киберпреступлений, финансовых преступлений, терроризма и транснациональной организованной преступности. В данной статье исследуется правовая природа цифровых доказательств, анализируются международные стандарты, регулирующие их сбор и допустимость, а также рассматриваются основные проблемы, возникающие в уголовном процессе. Особое внимание уделяется вопросам подлинности, достоверности, юрисдикции, защиты частной жизни и международного сотрудничества при получении электронных доказательств. Кроме того, анализируется законодательство Республики Узбекистан в сфере цифровых доказательств и предлагаются рекомендации по гармонизации национального законодательства с международными стандартами.

Ключевые слова: цифровые доказательства, уголовный процесс, киберпреступность, электронные доказательства, международное право, Будапештская конвенция, уголовное правосудие, кибербезопасность, допустимость доказательств, электронное расследование.

The digital transformation of modern society has fundamentally changed the methods by which crimes are committed, investigated, and prosecuted. Today, smartphones, computers, cloud storage systems, social media platforms, and electronic communications contain vast amounts of information that may serve as evidence in criminal proceedings. Consequently, digital evidence has become an essential component of modern criminal justice systems.[1] Unlike traditional forms of evidence, digital evidence possesses unique characteristics. It is highly fragile, easily alterable, transferable across borders within seconds, and often stored in decentralized digital environments.[2] These features create serious legal and procedural challenges concerning admissibility, authenticity, and reliability in criminal proceedings.

The growing number of cybercrimes, online fraud, digital terrorism, and transnational criminal networks has intensified the importance of effective regulation concerning electronic evidence. International organizations

[1] Susan W. Brenner, Cybercrime and the Law (Northeastern University Press, 2012), p. 45.
[2] Jonathan Clough, Principles of Cybercrime (Cambridge University Press, 2015), p. 144.

increasingly emphasize the necessity of harmonizing legal standards for collecting, preserving, and exchanging digital evidence among states.[3] This article analyzes the legal nature of digital evidence, examines international legal standards governing electronic evidence, identifies key challenges in criminal proceedings, and evaluates the legal framework of Uzbekistan in this field.

Digital evidence may be defined as information of evidentiary value stored or transmitted in digital form.[4] It includes emails and electronic correspondence, computer files and databases, social media communications, GPS and geolocation data, surveillance recordings, blockchain transaction records, metadata and cloud-stored information. Digital evidence differs significantly from physical evidence because it is intangible and highly dependent on technological infrastructure.[5] One of the most important characteristics of digital evidence is volatility. Electronic information may easily be modified, deleted, encrypted, or remotely destroyed. Therefore, timely preservation and forensic integrity are essential in criminal investigations.

Budapest Convention on Cybercrime: The Convention on Cybercrime adopted by the Council of Europe in 2001 remains the primary international legal instrument regulating electronic evidence and cyber investigations.[6] The Convention establishes procedural powers concerning: expedited preservation of stored computer data, production orders, search and seizure of computer systems, real-time traffic data collection, interception of electronic communications. The Budapest Convention also provides mechanisms for international cooperation and mutual legal assistance in obtaining digital evidence.

The United Nations increasingly recognizes the importance of electronic evidence in combating transnational cybercrime and terrorism. UN resolutions emphasize balancing cybersecurity measures with protection of human rights, privacy, and due process guarantees.[7]

One of the major legal problems concerns verification of authenticity. Courts must ensure that digital evidence has not been manipulated or altered.[8] Hash functions, chain-of-custody procedures, and forensic imaging are essential mechanisms for preserving evidentiary integrity.

[3] United Nations Office on Drugs and Crime (UNODC), Comprehensive Study on Cybercrime, 2013.
[4] Eoghan Casey, Digital Evidence and Computer Crime (Academic Press, 2011), p. 7.
[5] George L. Paul, Foundations of Digital Evidence (American Bar Association, 2008), p. 33.
[6] Convention on Cybercrime (Budapest Convention), Council of Europe, 2001.
[7] United Nations General Assembly Resolution No. 74/247, 2019.
[8] Eoghan Casey, Digital Evidence and Computer Crime, p. 56.

Digital evidence frequently crosses national borders. Cloud servers storing evidence may be located in foreign jurisdictions, creating conflicts concerning sovereignty and applicable law.[9] Traditional territorial principles of criminal procedure often prove ineffective in cyberspace. Obtaining electronic evidence frequently involves access to personal communications and private information. Excessive surveillance may violate privacy rights guaranteed under international human rights law.[10] Balancing criminal investigations with fundamental rights remains one of the most difficult legal challenges.

Artificial intelligence technologies increasingly influence criminal investigations. AI systems are capable of processing large volumes of digital information, facial recognition analysis, predictive policing, and automated evidence classification.[11] However, the use of AI raises serious concerns regarding algorithmic bias, transparency, accountability, and admissibility of AI-generated evidence.

Uzbekistan has undertaken reforms aimed at strengthening cybersecurity and regulation of electronic evidence. National criminal procedure legislation increasingly recognizes electronic information as admissible evidence in criminal proceedings.[12] Nevertheless, several issues remain unresolved: insufficient digital forensic expertise, limited technical infrastructure, lack of specialized cyber investigators, necessity for greater international cooperation. Further modernization of legislation remains necessary to ensure compatibility with international standards.

Recommendations

The following measures may significantly improve regulation of digital evidence: harmonization of procedural legislation with international standards, strengthening digital forensic institutions, developing specialized cybercrime investigation units, improving international cooperation mechanisms, adopting clear legal standards concerning AI-generated evidence, ensuring stronger protection of privacy and due process rights.

Conclusion: Digital evidence has become a central element of modern criminal proceedings. Its importance will continue to increase alongside technological development and digital globalization. Nevertheless, electronic evidence presents serious legal challenges concerning authenticity, admissibility, jurisdiction, and human rights protection. International legal cooperation,

[9] Marco Gercke, Understanding Cybercrime (ITU Publication, 2012), p. 78.
[10] European Court of Human Rights, Big Brother Watch v. United Kingdom, 2021.
[11] Richard Susskind, Online Courts and the Future of Justice (Oxford University Press, 2019), p. 210.
[12] Criminal Procedure Code of the Republic of Uzbekistan, provisions concerning electronic evidence.

harmonization of legislation, and modernization of procedural safeguards remain essential for ensuring effective and lawful use of digital evidence in criminal justice systems.

References

Susan W. Brenner, Cybercrime and the Law (Northeastern University Press, 2012), p. 45;
Jonathan Clough, Principles of Cybercrime (Cambridge University Press, 2015), p. 144;
United Nations Office on Drugs and Crime (UNODC), Comprehensive Study on Cybercrime, 2013;
Eoghan Casey, Digital Evidence and Computer Crime (Academic Press, 2011), p. 7;
George L. Paul, Foundations of Digital Evidence (American Bar Association, 2008), p. 33;
Convention on Cybercrime (Budapest Convention), Council of Europe, 2001;
United Nations General Assembly Resolution No. 74/247, 2019;
Eoghan Casey, Digital Evidence and Computer Crime, p. 56;
Marco Gercke, Understanding Cybercrime (ITU Publication, 2012), p. 78;
European Court of Human Rights, Big Brother Watch v. United Kingdom, 2021;
Richard Susskind, Online Courts and the Future of Justice (Oxford University Press, 2019), p. 210;
Criminal Procedure Code of the Republic of Uzbekistan, provisions concerning electronic evidence.