Latin American Journal of Education
www.lajoe.org

DIGITAL FORENSICS IN THE INVESTIGATION OF TRANSNATIONAL CRIMES: ISSUES OF ADMISSIBILITY OF EVIDENCE AND INTERNATIONAL COOPERATION (THE CASE OF THE REPUBLIC OF UZBEKISTAN)

https://doi.org/10.5281/zenodo.19535226

Student of Tashkent International University
Rizaeva Zarina
Scientific advisor: **Turimbetov R.M.**

Аннотация: *В статье рассматриваются вопросы использования цифровой криминалистики в расследовании транснациональных преступлений. Анализируются понятие и особенности цифровых доказательств, а также проблемы их допустимости, включая аутентичность, целостность и законность получения. Особое внимание уделяется международно-правовому регулированию, в том числе Budapest Convention on Cybercrime, и роли INTERPOL в обеспечении сотрудничества государств.*

Ключевые слова: *Цифровая криминалистика; цифровые доказательства; транснациональная преступность; допустимость доказательств; судебная экспертиза; киберпреступность; международное сотрудничество; Budapest Convention on Cybercrime; INTERPOL; Республика Узбекистан*

Annotatsiya: *Maqolada transmilliy jinoyatlarni tergov qilishda raqamli kriminalistikadan foydalanish masalalari ko‘rib chiqiladi. Raqamli dalillarning tushunchasi va xususiyatlari, shuningdek ularning maqbulligi bilan bog‘liq muammolar — jumladan, autentiklik, yaxlitlik va qonuniy yo‘l bilan olinishi masalalari tahlil qilinadi. Xalqaro-huquqiy tartibga solishga alohida e’tibor qaratilib, xususan, Kiberjinoyatchilik to‘g‘risidagi Budapesht konvensiyasi hamda davlatlar o‘rtasidagi hamkorlikni ta’minlashda INTERPOLning roli yoritiladi.*

Kalit so'zlar: *Raqamli kriminalistika; raqamli dalillar; transmilliy jinoyatchilik; dalillarning maqbulligi; sud ekspertizasi; kiberjinoyatchilik; xalqaro hamkorlik; Kiberjinoyatchilik to‘g‘risidagi Budapesht konvensiyasi; INTERPOL; O‘zbekiston Respublikasi*

Abstract: *The article examines the use of digital forensics in the investigation of transnational crimes. It analyzes the concept and specific features of digital evidence, as well as the issues of its admissibility, including authenticity, integrity, and legality of acquisition. Special attention is given to international legal regulation, including the*

Latin American Journal of Education
www.lajoe.org

Budapest Convention on Cybercrime, and the role of INTERPOL in facilitating cooperation among states.

Key words: *Digital forensics; digital evidence; transnational crime; admissibility of evidence; forensic examination; cybercrime; international cooperation; Budapest Convention on Cybercrime; INTERPOL; Republic of Uzbekistan*

In the context of globalization and the development of information and communication technologies, transnational crime is taking on new forms due to the use of digital tools and platforms. Cybercrime, illegal data trafficking, and other types of transnational criminal activity complicate the processes of detection and investigation. The growth of transnational crime, including cybercrime and illegal data circulation, is confirmed by international studies, in particular reports of the United Nations Office on Drugs and Crime, which note an increase in the share of crimes committed using digital technologies.

Digitalization has led to the emergence of new types of evidence existing in electronic form: correspondence, metadata, data from social networks, and cloud services. Under these conditions, digital forensics becomes a key tool for their identification, recording, and analysis. However, the characteristics of digital data, including their variability and dependence on technical conditions, create problems of reliability and admissibility in judicial proceedings.

Legal regulation in this area significantly lags behind technological development: the absence of unified standards for handling digital evidence remains one of the key problems. In this regard, the recommendations of the European Union Agency for Cybersecurity are aimed at developing unified approaches to digital forensics and ensuring the reliability of digital evidence.

The purpose of this article is to analyze the role of digital forensics in the investigation of transnational crimes and to identify issues of admissibility of digital evidence and international cooperation.

To achieve this goal, the following tasks are set:

- to раскрыть the concept of digital forensics;
- to analyze the international legal framework;
- to identify problems of admissibility of digital evidence;
- to study the features of international cooperation;
- to identify gaps in the legislation of the Republic of Uzbekistan.

Digital forensics is a branch of forensic science aimed at identifying, seizing, preserving, investigating, and analyzing information in digital form for use as evidence in criminal and other judicial proceedings. In scientific literature, digital forensics is considered

Latin American Journal of Education
www.lajoe.org

as a set of methods for identifying, preserving, and analyzing digital data for the purpose of their use as evidence (Casey E.).

There is no unified legal definition at the international level, but within the framework of the Budapest Convention on Cybercrime, the term "computer data" is defined as any information that can be processed in a computer system, including programs, which essentially forms the basis for understanding digital evidence. In the doctrinal approach, digital forensics is considered as a set of scientifically grounded methods for working with such data for procedural use.

Digital evidence includes various data, in particular:

- electronic correspondence (messengers, e-mail);
- metadata (time of creation, modification, transmission of information);
- IP addresses and other network identifiers;
- data stored in cloud services and on remote servers;
- information from social networks and digital platforms.

The importance of digital forensics is conditioned by the fact that in the era of digitalization, these data increasingly become important evidence for the investigation of cross-border crimes, including cybercrime, financial fraud, and illegal information trafficking.

However, digital evidence has a number of specific characteristics that distinguish it from traditional evidence. First, it is characterized by a high degree of variability, which requires the use of special methods of fixation and preservation. Second, this data depends on the technical environment (software, hardware, network infrastructure), which affects the possibility of its extraction and interpretation. Third, it is characterized by increased complexity of verification, since establishing authenticity and integrity requires special procedures, in particular to ensure the continuity of storage (chain of custody).

International legal regulation of digital forensics is formed mainly within the framework of combating cybercrime and transnational crime. The key international act in this area is the Budapest Convention on Cybercrime of 2001, which provides key mechanisms for combating crimes in the digital environment, including the preservation and seizure of computer data, the mechanism of expedited preservation of information, as well as the provision of mutual legal assistance between states. At the same time, scientific literature points to a number of its shortcomings: a limited circle of participants, insufficient regulation of cross-border access to data, and the need to adapt to modern technological challenges. In this regard, the initiatives of the United Nations to develop a universal convention on cybercrime are of particular importance, which indicates the insufficiency of existing international legal mechanisms.

Latin American Journal of Education
www.lajoe.org

The Convention establishes such important instruments as the preservation of computer data, their seizure, search and interception, and also provides for procedures for mutual legal assistance between states. Of particular importance are provisions aimed at ensuring prompt access to data, including the mechanism of expedited preservation of information (expedited preservation of data), which is critically important in conditions of their high variability.

A significant role in coordinating international interaction is played by INTERPOL, which ensures the exchange of operative information, the development of digital forensics, and support for cross-border investigations. Through specialized units and databases of INTERPOL, states are able to promptly exchange digital evidence and coordinate the actions of law enforcement agencies.

The practice of the International Criminal Court also demonstrates the growing importance of digital evidence in the investigation of international crimes, including war crimes and crimes against humanity. The Court активно uses digital materials such as video recordings, satellite images, and data from open sources (OSINT — Open Source Intelligence), which requires the development of standards for their assessment, authenticity, and admissibility.

One of the key problems of international legal regulation is cross-border access to data. In conditions where information is stored on servers located in different jurisdictions, there is a need to obtain permissions from foreign states, which significantly slows down the investigation process. Despite the existence of mutual legal assistance mechanisms, their application often does not meet the requirements of promptness.

The exchange of digital evidence between states is also complicated by the absence of unified standards for their collection, fixation and storage. Differences in procedural requirements may lead to the recognition of evidence as inadmissible in another jurisdiction.

An additional complexity is the issue of jurisdiction. The transnational nature of crimes committed in cyberspace makes it difficult to determine the state having the right to investigate and prosecute. This leads to conflicts of jurisdiction and reduces the effectiveness of international cooperation.

Thus, despite the existence of international legal instruments, the regulation of digital forensics remains fragmented and requires further unification, especially in terms of standards for working with digital evidence and mechanisms of cross-border access to data.

The admissibility of digital evidence is one of the key problems of modern law enforcement practice, since its use requires compliance with both procedural and technical standards. In criminal proceedings, the admissibility of evidence is determined by its legality, reliability, and relevance, which fully applies to

Latin American Journal of Education
www.lajoe.org

digital data (Ashworth A., Redmayne M.). Unlike traditional evidence, digital data is subject to changes, depends on the technical environment, and requires special methods of verification.

The first problem is establishing the authenticity of digital evidence. The need to prove that the presented data is genuine and has not been altered is complicated by the possibility of its editing without visible traces. In this regard, methods of digital forensics are of particular importance, including the use of hash functions that make it possible to confirm the immutability of data.

The second problem is ensuring the integrity of evidence. Any violation of the procedure for seizure, storage, or transfer of digital data may lead to its distortion, which calls into question its evidentiary value. In international practice, special attention is paid to compliance with procedures ensuring the integrity of digital evidence. Thus, the recommendations of the National Institute of Standards and Technology provide for mandatory documentation of all stages of working with digital data within the framework of the principle of continuity of storage (chain of custody – a documented chronological sequence of the collection, transfer, analysis, and storage of materials or evidence).

The third significant problem is the legality of obtaining digital evidence, especially in a cross-border context. Data obtained in violation of national legislation or without compliance with procedures of international legal assistance may be recognized as inadmissible in court. This is especially relevant in cases where information is extracted from servers located in another jurisdiction.

The fourth problem is the complexity of procedural evaluation of digital evidence. Judicial authorities often face the need to assess technically complex information, which requires the involvement of experts and increases the dependence of the court's decision on the quality of the conducted examination. At the same time, the absence of unified standards of forensic digital examination may lead to different interpretations of the same data.

An additional problem is the risk of falsification of digital evidence, including the creation of fake messages, modification of metadata, and the use of deepfake technologies (a method of content synthesis based on machine learning and artificial intelligence). This increases the requirements for procedures of authenticity verification and enhances the importance of qualified forensic examination.

Thus, the admissibility of digital evidence directly depends on compliance with a set of requirements, including their lawful acquisition, ensuring integrity, confirmation of authenticity, and proper expert evaluation. The absence of unified standards in this area significantly reduces the effectiveness of their use in the investigation of transnational crimes and requires further improvement of legal regulation.

Latin American Journal of Education
www.lajoe.org

In the Republic of Uzbekistan, legal regulation of digital evidence is carried out mainly within the framework of criminal procedural legislation. Significant changes in this area have been introduced in recent years, which indicates the gradual adaptation of the legal system to the conditions of digitalization.

According to the provisions of the Criminal Procedure Code of the Republic of Uzbekistan, evidence is recognized as any factual data on the basis of which the circumstances of the case are established, including audio and video recordings and other documents. At the same time, the legislation directly establishes the concept of digital evidence. In particular, in accordance with Article 204² of the Criminal Procedure Code of the Republic of Uzbekistan, digital evidence is recognized as electronic data containing information about circumstances relevant to the case, including files, audio and video recordings, as well as data posted on the Internet.

The procedure for obtaining such evidence is also of great importance. The law provides that electronic data may be seized during investigative actions, including search, seizure, inspection, as well as obtained from telecommunication networks and the Internet. At the same time, evidence must be collected in compliance with the established procedural form, since violation of the procedure for obtaining it entails its recognition as inadmissible.

Particular attention is paid to the institution of admissibility of evidence. In accordance with the norms of the Criminal Procedure Code of the Republic of Uzbekistan, evidence is recognized as admissible only if it is obtained by lawful methods, and data obtained in violation of procedural requirements or the rights of participants in the process are subject to exclusion from the evidentiary base. This provision fully applies to digital evidence.

A significant role in working with digital evidence is played by forensic examination. According to Article 172 of the Criminal Procedure Code of the Republic of Uzbekistan, an examination is assigned in cases where special knowledge in the field of science and technology is required to establish the circumstances of the case. In the context of digitalization, this includes conducting computer-technical and other types of digital examinations aimed at analyzing electronic data.

At the same time, despite the existence of a regulatory framework, the regulation of digital evidence in Uzbekistan remains insufficiently detailed. Although amendments were introduced in 2024 aimed at improving work with digital evidence, including their consolidation in procedural codes, in practice significant problems remain.

The main ones include:

– the absence of clear procedures for ensuring the integrity of digital data (chain of custody);

– insufficient regulation of methods of digital examination;

Latin American Journal of Education
www.lajoe.org

– limited mechanisms of cross-border access to data;

– the absence of unified standards for evaluating digital evidence in court.

Thus, the legislation of the Republic of Uzbekistan in the field of digital evidence is at the stage of formation and development. Despite the consolidation of basic concepts and procedures, further improvement of legal regulation requires deeper integration of international standards and the development of specialized norms taking into account the specifics of digital forensics.

The analysis of international practice and national legislation of the Republic of Uzbekistan allows concluding the need for further improvement of legal regulation of digital forensics and handling of digital evidence.

First of all, it seems appropriate to develop and implement unified procedural standards for working with digital evidence, including the procedure for their seizure, fixation, storage, and examination. Particular attention should be paid to the normative consolidation of the principle of continuity of storage (chain of custody), as well as to establishing requirements for mandatory recording of hash values, which will ensure the integrity and reliability of digital data.

An important direction is the harmonization of national legislation with international standards, including the provisions of the Budapest Convention on Cybercrime. This will increase the effectiveness of international cooperation and simplify procedures for the exchange of digital evidence in the investigation of transnational crimes. At the same time, it is necessary to improve mechanisms of cross-border access to data, including simplification of procedures of international legal assistance and development of cooperation with international organizations, in particular INTERPOL.

No less important is the development of the institution of forensic digital examination. It is necessary to develop unified methodologies for conducting computer-technical examinations, introduce unified standards of digital examination, and train qualified specialists in the field of digital forensics. Additionally, it seems necessary to adopt departmental instructions of the Prosecutor General's Office and the Ministry of Internal Affairs of the Republic of Uzbekistan regulating the procedure for working with digital evidence. This will improve the quality of expert conclusions and reduce the risk of erroneous interpretation of digital data.

In addition, it is necessary to introduce clear criteria for assessing the admissibility of digital evidence in judicial practice, including requirements for their authenticity, integrity, and legality of obtaining, which will ensure uniformity of law enforcement and increase the level of protection of the rights of participants in the process.

The conducted analysis has shown that digital evidence has specific

Latin American Journal of Education
www.lajoe.org

characteristics, including variability, dependence on the technical environment, and complexity of verification, which significantly affects their evidentiary value. In this regard, issues of authenticity, integrity, and legality of obtaining such data acquire fundamental importance for their admissibility in judicial proceedings.

International legal regulation in this area, in particular the provisions of the Budapest Convention on Cybercrime, forms the basis for interaction between states, but does not ensure full unification of approaches to handling digital evidence. The practice of international cooperation, including the activities of INTERPOL, demonstrates significant potential, but at the same time reveals problems caused by differences in national legal systems and difficulties of cross-border access to data.

The study of national legislation of the Republic of Uzbekistan has shown that, despite the existence of basic norms regulating the use of digital evidence, legal regulation remains insufficiently detailed. The absence of unified standards for fixation, storage, and evaluation of digital data, as well as limited mechanisms of international interaction, reduce the effectiveness of their use in law enforcement practice.

Under these conditions, the improvement of legal regulation should be comprehensive and include the introduction of unified procedural standards for working with digital evidence, the development of the institution of forensic digital examination, the adoption of departmental regulations, and active harmonization of national legislation with international standards. Particular importance is also attached to improving the qualifications of specialists and developing technical infrastructure ensuring reliable work with digital data.

Thus, further development of digital forensics and improvement of legal mechanisms for handling digital evidence are a necessary condition for increasing the effectiveness of investigation of transnational crimes and ensuring fair justice in the context of digital transformation.

Latin American Journal of Education
www.lajoe.org

LIST OF REFERENCES:

1. Budapest Convention on Cybercrime. Budapest, 2001. // https://rm.coe.int/1680081561
2. United Nations Office on Drugs and Crime. Comprehensive Study on Cybercrime. New York, 2013. // https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
3. INTERPOL. Global Cybercrime Strategy. Lyon, 2022. // https://www.interpol.int/en/content/download/18350/file/Global Crime Trend Summary Report EN.pdf
4. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. Academic Press, 2011. // https://rishikeshpansare.wordpress.com/wp-content/uploads/2016/02/digital-evidence-and-computer-crime-third-edition.pdf
5. National Institute of Standards and Technology. Guide to Integrating Forensic Techniques into Incident Response (SP 800-86). 2006. // https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf
6. Criminal Procedure Code of the Republic of Uzbekistan. // https://lex.uz/docs/111463
7. Ashworth A., Redmayne M. The Criminal Process. Oxford University Press, 2010. // https://pbio.akademia.mil.pl/wp-content/scans/2024/CYBERBEZPIECZENSTWO/OCR/26672_III_OCR.pdf
8. OSINT — Open Source Intelligence // https://osintframework.com/