Impact Factor: 9.9 ISSN-L: 2544-980X

The Concept of Electronic Digital Evidence and its Role in the Process of Proof

Badalboev Feruz Yusufovich [1]

Annotation: The article analyzes the current state of the concept of electronic digital evidence, its significance, types, and the role of the preliminary investigation bodies in the practical activities of proving in criminal cases, the study and analysis of digital traces, their use as evidence, and makes a number of proposals for amendments to current legislation

Key words: criminal process, electronic evidence, electronic means of proof, electronic media.

The measures taken in recent years to widely introduce modern technologies in the activities of courts have allowed citizens and business entities to liberalize their access to the courts to protect their rights and interests, increase access to justice in general, and ensure openness and transparency in the activities of courts.

Today, globalization on a global scale, in the era of information and communication technologies, requires development in step with the fast-paced era. In the era of information and communication technologies, with the emergence of new types of evidence, it is necessary to improve the industry in accordance with this[2].

The development of electronic digital technologies, the widespread use of the Internet, and the availability of personal digital devices facilitate the commission of cybercrime and create problems in the detection of such crimes. Currently, it is not necessary to be in any country to commit a crime, a personal computer or smartphone connected to the internet is enough to commit a crime in the territory of any country. Such a situation creates significant difficulties in identifying criminals.

In this regard, in recent years, the need to develop a regulatory framework that allows for the full use of various technical means and software packages for identifying, recording, and retrieving digital traces in the memory of electronic devices has become increasingly relevant[3].

The difference from other forms of electronic digital evidence is that digital evidence can be created almost instantaneously, with a direct press of several buttons, or even without the direct involvement of a person. One of the definitions of electronic digital evidence is the interpretation of a combination of data stored on a computer (when it is on a hard disk), or in motion (network communications). There are also other universally accepted definitions given by leading organizations and scholars that serve to describe the theory of "electronic digital evidence."

A duplicate of electronic digital evidence ("Duplicate Digital Evidence") is an exact copy of all the data available on the original object - a precise replication of the information present on the initial data objects. The Association of Chief Police Officers (ACPO) defines computer electronic evidence as information and data of investigative significance that is stored on a computer or transmitted using a computer.

The crime scene refers to the data found on digital devices such as computers (hard drives) or storage media (flash drives) discovered at the location of the crime. The mere presence of "electronic digital

[1] Deputy Head of the Organizational Department of the Ministry of Internal Affairs of the Republic of Uzbekistan, Head of the Department of Legal Support

evidence" (in the form of data stored on a digital device) at the crime scene may not necessarily qualify it as admissible evidence[4].

According to the most widely accepted definition in the field of criminal procedure and criminology, electronic digital evidence is any information in digital form that has the force of evidence and can be used as reliable evidence in investigation and in court.

A.B. Sabirbaeva, in her scientific work, defines "electronic evidence" as follows: "electronic evidence is information stored or transmitted in digital form, directly or indirectly related to the commission of a crime, reflecting the circumstances of the crime committed, seized and formalized in accordance with the norms of the Criminal Procedure Code".[5]

In his scientific work, Professor A.A. Matchanov puts forward the idea that "electronic (digital) data containing information about circumstances relevant to the case, including electronic files, audio and video recordings, and data stored on the Internet are electronic (digital) evidence".[6]

In our view, electronic digital evidence is any information created, processed, stored, or transferred digitally that can be accepted by the investigation and the court as reliable evidence, as well as copies of digital data that can be accepted by the investigator and the court as evidence. At the same time, the concept of written and digital evidence has been introduced into the criminal procedural legislation of the Republic of Uzbekistan.

Article 81 of the Criminal Procedure Code enshrines digital evidence as evidence. They exist only from a legal standpoint, which positively affects the investigation of the criminal case by the investigator and the inquiry officer of the criminal process. In Article 140 of the Criminal Procedure Code, Article 157 "Search of Electronic Data" is limited to describing the provisions of the concept of "seizure of electronic data," and currently, when obtaining electronic digital evidence, the investigator, investigator, and prosecutor must possess special knowledge and the necessary equipment to obtain information of forensic significance.

Due to the rapid development of electronic means and the growing volume of important types of information of electronic digital evidence, it is difficult to give an accurate and limited classification of all potential sources of digital evidence, but at the same time, the denial of their significance in the criminal process, as a modern and effective type of evidence, leads to a change in the legal aspect. Based on practical experience, various examples of digital information sources can be cited and their types and current state can be identified. Based on practical experience, we believe it is advisable to divide sources of electronic digital evidence into the following types based on the source of their formation:

- the main records of transactions - they include all purchases, sales and other contractual agreements concluded in a cashless environment;
- basic business records - they include all of the above, as well as all documents and information (contracts, agreements sent by email, etc.) that may be necessary to comply with legal and regulatory requirements;
- postal traffic - e-mails can provide important evidence of official and unofficial communication;
- recordings stored by third parties, such as a cloud data provider (cloud data warehouse);
- separate individual personal computers;
- separate mobile phones / smartphones, tablets / devices, etc.;
- Data carriers - most computer users archive their actions completely or partially on external media, such as CD discs, digital devices.
- universal discs, magnetic strips, external hard drives, memory cards and universal flash drives;

- access control logs - all digital devices, except for the most basic computer systems, require a password or authentication device before allowing access;
- all computers have files that help determine how the operating system should work;
- Internet activity magazines;
- antivirus "journals"
- The above-mentioned logs are related to logs created by enterprise antivirus software devices, which record the detection and destruction of viruses.
- attack detection logs - larger computer systems often use attack detection systems as part of security, designed to detect and prevent various violati
- backup carriers - all computer systems must have backup procedures that ensure quick recovery after possible complete deletion or software malfunction;
- telephone logs - carriers usually have a wide range of opportunities to record the activity of using the subscriber number;
- telephone recordings - data obtained from current control, listening and recording of conversations of certain persons;

E-digital evidence is valuable information and evidence in itself is very sensitive in nature, as it can be easily altered, forged, or destroyed as a result of misuse or prior seizure. Therefore, the investigator, investigator, prosecutor, and specialist working directly with digital traces must have a unique understanding and knowledge of identifying, recording, and seizing information related to digital evidence.

In this regard, the information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence (Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence), which is a true translation of the international standard ISO/IEC 27037:2012, is of scientific and practical interest to scientists and practitioners, during its study, investigators can obtain information, on the basis of which it is possible to determine the reliability of electronic digital evidence.

Currently, the proper use of electronic digital evidence in the process of investigation and trial is insufficient, primarily due to the fact that this process is not simply regulated by law, as well as the lack of a legal framework for the collection and storage of digital evidence, as described above, as well as their subsequent use, including when it is necessary to conduct a forensic examination for the analysis of digital evidence.

At the same time, it should be noted that, in our opinion, it is not advisable to include a separate article for digital (electronic) evidence in Article 81 of the Criminal Procedure Code, as it is very difficult to determine the volume of digital (electronic) evidence (information of digital forensic significance), at least there is no consensus on this matter, moreover, the very rapid development of digital technologies, in our opinion, has lost its relevance and required amendments, which may complicate law enforcement practice.

Furthermore, taking into account the practical activities and experience of various law enforcement agencies, the current criminal procedure legislation should enshrine general rules to ensure an effective method of storing electronic digital evidence, while specific methods of work should be regulated by departmental and interdepartmental orders and methodological instructions, as this does not fall within the scope of criminal procedural regulation.

Currently, general rules for storing electronic digital evidence are applied based on criminal procedural requirements. While this statement is true, it does not take into account the specifics of digital forensic information and digital evidence.

There is no single competent authority that is engaged in the search, recording, verification, analysis and presentation of evidence in digital form. Various law enforcement agencies (the Prosecutor's Office, the Ministry of Internal Affairs, the State Security Service, and a number of other expert units) are involved in this, but neither the Criminal Procedure Code nor any other legal sources specify which bodies investigate and study digital evidence.

Modern technological achievements and digital innovations are increasingly impacting various spheres of society, including the judicial and investigative systems. Digitalization of criminal proceedings is one of the directions for the development of the legal system, which can significantly increase the efficiency and popularity of justice, as well as ensure the transparency and speed of the process. In recent years, digital technologies have been actively used in criminal proceedings, bringing new developments and changing the traditional methods of work of the judicial and investigative system.

References:

1. REGULATION "On the Department for the Implementation and Development of Information and Communication Technologies." October 05, 2015
2. Vekhov, V. B. Electronic evidence: problems of theory and practice / V. B. Vekhov // Legal order: history, theory, practice. - 2016. - No. 4 (11). - C. 46-50.
3. Cherdantsev A. Yu. The concept of digital evidence, the modern state and their role in the evidentiary process // Legal science and practice. 2019. No. 15 (4). C. 55-60.
4. Saburbayeva A.B. Improving the Methodology of Fraud Crime Investigation. Tashkent, 2022. - C. 56 б.
5. Matchanov A.A. Investigation of Cybercrime / Textbook of the Academy of the Ministry of Internal Affairs: 2019. 108 p.
6. Polyakov M.P., Smolin A.Yu. Conceptual Analysis of the Phenomenon of Electronic Evidence // Legal Science and Practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia. 2019. No. 2 (46). P. 135-145.
7. Marfitsin P.G. Some approaches to the definition of the concept of "electronic proof" // Legal science and practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia. 2017. No. 3 (38). C. 106-109.
8. Alexandrov, A.S. On the reliability of "electronic evidence" in criminal proceedings / A.S. Alexandrov, S.I. Kuvichkov // Criminalist's Library. Scientific journal. - 2013. - No. 5 (10). - C. 76 - 84.