USING DIGITAL DATA AS EVIDENCE IN CRIMINAL INVESTIGATIONS

Axmedova Kamola Zoirjon qizi
Tashkent State University of Law
kamolaaxmedova99@gmail.com

Abstract

Digital technologies have become an integral part of human lifestyles by the 21st century. As a result of the development of technology, new types of crime began to appear in the human world. These processes are leading to a high-rate increase in the trend of using digital data as evidence in crime investigations. This article will talk about digital data, the possibilities of their use, as well as issues of evaluating them as evidence. In addition, the article provides a comparative analysis of the legislative norms governing electronic evidence in Uzbekistan, as well as the norms of international law. At the end of the article, conclusions are made about the prospects for using digital data as evidence.

Keywords: Electronic evidence, Digital information, Cybercrime, Cyber attacks, Digital revolution.

I. Introduction

It is known to us that today, research work is being carried out through modern devices, where digital technologies cover the entire universe, and even on other planets from Planet Earth, resulting from the achievements of digital technologies. It is seen from this that through digital technologies, humanity is developing and perfecting further, while, through these technologies, new types of crime have also begun to appear in the criminal world. As we follow social networks that have been deceived through online trading, or information about individuals whose money was stolen from their plastic card has become much more abundant today. A new type of crime called cybercrime has entered the criminal world. Currently, Uzbekistan is ranked 47th among the countries of the world for the occurrence of cyber attacks. Considering that there are 193 independent countries

in the world, we must be aware that 47 places are far ahead and that a new type of crime poses a great threat to our country.

Until this century, when there was a “bourgeois revolution”, an industrial revolution in history, today the” digital revolution “is changing every sphere of our society, and these processes are taking their toll even on the criminal sphere. The development of digital technologies poses problems with the introduction of new concepts and terms in theory and practice. In particular, if in the 90s of the last century the terms “computer evidence” or “Internet evidence” were widely used, today the concepts of “electronic evidence” or “digital evidence” and issues related to the definition of their legal status are the subject of heated debate among legal scholars [1].

The article analyzes the criminalistic aspects of the use of digital data as evidence in the investigation of crimes, theoretically illuminating the problems of using digital data as evidence and the conditions for their assessment as evidence, as well as providing conclusions, suggestions and recommendations aimed at improving legislation and practice in this area.

II. Methodology

The methodological basis of this article is the general scientific and special methods of knowledge, scientific research of domestic and foreign authors, National Criminal Procedure legislation of the Republic of Uzbekistan, as well as the relevant legislation of foreign countries. In particular, the method of materialistic dialectics is used, which is based on the objective analysis of reality, allows you to consider phenomena in interdependence and connection, in their dynamics and development. Among the general scientific methods of research, historical, logical, sociological methods are also used, which make it possible to determine the most important naturalness and express it in a scientific, abstract-theoretical form. In particular, the method of historical research makes it possible to track the history of formation and development of digital data as evidence. The logical method makes it possible to conduct research on the basis of the laws of logic, determining the order, sequence

of development of legal concepts and categories. The sociological research method the problem under study is related to the use of relevant statistics.

III. Results

In digital devices citizenship from stored digital information, administrative, economic and criminal proceedings increasing the need to use in the process of proof is getting. In particular, at the pre-trial and trial stages of the case, it remains relevant to determine the ties between the parties, ties and establish standards of universal importance in the collection, verification, storage and assessment of digital evidence of significance for the case [2].

It is impossible to correctly solve the practice associated with them without understanding the peculiarities, complex composition and mechanism of digital evidence, which affects procedural processes at the stages of conducting a case before trial and in court. In terms of proof, digital evidence has a much wider scope than material (traditional) evidence. They have the characteristics of sensitivity and mobility, and the collection, inspection, storage and evaluation processes require special training and tools [3].

In a 2008 definition by the National Institute of Justice of the United States, digital evidence – derived from digital devices, stored or transmitted, is recognized as the value of information or data for investigation [4].

Analyzing the above, the concept of digital information is a concept with a wide scope. It requires both theoretical and practical knowledge to collect, examine, evaluate as evidence. Below we will briefly talk about the questions that arise on the topic and their solution by discussing this topic.

IV. Discussion

Information is an important aspect of various spheres of human activity, and the current period is characterized by the general availability of a large amount of information. In general, information is the process of exchanging information between content - rich information transmitted by people orally, in writing, or otherwise, including people, an individual, and a technical device, or just a technical

device. Information is an object of not only transmission, but also storage and processing (transformation, calculation).

The concept of" digital information "is a general concept in relation to" computer data", since it describes the variety of all forms in which information used by modern computing, telecommunications and other technical devices can exist and be transmitted.

Digital data is data converted to digital code. It is set by digital recording, with the help of which the signals registered on the carrier are converted into a sequence of code (digital) combinations of impulses (signals). Information is also transmitted through signals, which, unlike a message, are an external structure of information intended for transmission [5].

In traditional criminalistics, just as material evidence has its own characteristics, so do digital evidence. However, these characteristics are markedly different from the characteristics of traditional arguments.

Features of digital evidence:

- Invisibility;
- Complex composition;
- The clumsiness of interpretation.

Over the past 15 years, serious problems have begun to arise in the field of computer criminology. A sharp increase in the volume of digital evidence, an increase in the use of encryption, the creation of new technologies that lead to the progressive disappearance of digital evidence (for example, temporary), and among lawyers, prosecutors expect not only to prove the evidence on the defendant's computer, but also to prove that they belong to the defendant [6].

The general task of the subjects involved in the opening and investigation of crimes is to collect evidence confirming the guilt of the individual. Such evidence is generated from information that can be obtained in the manner prescribed by law. Information is perceived by the subject of Investigation as an objective feature of the objects of surrounding reality in the form of a trace (trace information) as a cluster of information directly or indirectly related to the crime phenomenon. Digital

traces, in turn, can be converted into a certain type of Criminal Procedural evidence-electronic evidence. In the Criminal Procedure legislation of Uzbekistan, today there are no norms governing the concept of electronic or digital evidence, its acquisition, collection, assessment as evidence, but research is carried out by scientific scientists in connection with digital evidence.

In addition to storage devices, the computer also has software, which also serves as a source of digital information due to its storage of digital information. The storage feature of the software is preferable to device sources. Because the software has the property of storing data in any case. Let's talk about Krenar Lusha Casey as an example.

Krenar Lusha was arrested by the United Kingdom based on his internet search sample. When his laptop was examined, it was found that he had downloaded 4,300 GM manuals to make explosives and search belts. When they searched his apartment for an additional investigation, the police also managed to find 71.8 l of gasoline, potassium nitrate and a live rifle cartridge. He also used the laptop to talk to people through Microsoft Network, describing himself as a terrorist or sniper. He showed himself to be a man who wanted to see the murder of Jews and Americans. These conversations were taken from his computer and used as digital evidence in court. Digital criminalistics once again helped solve the case [7].

As we observe keys in relation to Krenar Lusha, the evidence that served as the primary source of her crime is the digital data contained in her computer. One of the small problems with digital data was that we spoke above about the possibility of their change. Now we will focus on the issues of their collection in order to recognize digital data as evidence in court.

Digital data collection is the process of electronically collecting data using existing technologies such as smartphones, tablets and other digital devices that store data in themselves.

According to Article 95 of the Code of Criminal Procedure of the Republic of Uzbekistan “every argument should be evaluated in terms of involvement, acceptability and reliability of work."There is no such thing as the introduction of

the concept of digital evidence into Criminal Procedure Law. When the concept of electronic (digital) evidence comes into our legislation, the question of evaluating this evidence also comes to the fore.

To this day, the conditions for evaluating evidence are clear to us, but we do not have a clear idea of digital data as well as the conditions for evaluating them as evidence.

In 2017, the Harmonized Model for Digital Evidence Admissibility Assessment (HM-deaa) was developed by Antvi-Boasiako (Antwi – Boasiako) and Venter (Venter) on the technical and legal requirements of digital evidence acceptability. This model shows the following three stages of evaluating digital evidence.

a) evaluation of the acceptability of digital evidence:

At this stage, the compliance with procedural legislation and international standards and their importance in obtaining digital evidence is assessed criminally.

b) Digital Evidence Review

At this stage, the integrity of digital evidence, that is, compliance with examination procedures and tools, is assessed when obtaining, storing and analyzing them. The aim of this is to verify that scientifically based principles have been adhered to in finding, preserving and analyzing evidence, to ensure the quality of work and to build confidence in the results. At the same time, when working with digital evidence and researching them, it is also taken into account that standards are followed (for example, that digital criminalistics tools have undergone certification, reliability and correct operation have been confirmed, tested before use).

c) decision on the acceptability of digital evidence.

At this stage, the validity, integrity and reliability of digital evidence are evaluated based on the results of the second stage. For example, methods and tools for obtaining digital evidence are evaluated in terms of reliability, and expert testimony is compared . In order for the results to be deemed valid, they must be interpreted impartially, and information about errors, inaccuracies, and limitations must be disclosed [8].

The ISO / IEC 27037 standard provides harmonized and universally accepted methodologies to ensure the integrity and validity of digital evidence. It also serves to facilitate digital evidence exchange between jurisdictions through consistency of requirements and procedures.

Conclusion

The criminalistic aspects of the use of digital data as evidence in the investigation of crimes as a result of research carried out and studied in the writing of the article include our scientific-theoretical conclusions on the solution of problems and shortcomings encountered in science and in practice, proposals and recommendations aimed at improving current legislation and improving the effectiveness of:

The scientific work of Uzbek scientists, studied and analyzed above, is not yet enough to conclude that it fully covers the sources regarding the use of digital data as evidence in the investigation of crimes. Therefore, the types of digital sources of information and the possibilities of their use as evidence are very wide, therefore, the formation of processes for carrying out research on each type of digital sources of information, as well as a digital forensic examination of each type or group of digital sources of information, a number of Uzbek-language resources, that is, scientific and practical training manuals for each, in order to correctly write the conclusions of the examination and avoid errors and shortcomings in the process of research, it is recommended to formulate samples of conclusions regarding the types of digital forensics and develop new textbooks that form the expanded theoretical sources of Digital Forensics in itself.

Many scientific articles, literature on this field are written in a foreign language, due to the fact that cybercrime has not so much entered our country. Looking at Foreign practice in the development of the scientific-theoretical framework for the use of digital data as evidence in the investigation of crimes, it is recommended to establish the translation into Uzbek of literature, textbooks, teaching aids written in a foreign language and other documents directly related to foreign practice in order to apply those found to be effective in their practice.

Despite the fact that the number of cybercrime is increasing day by day, no legal basis for digital evidence has been created in criminal law. For this reason, it is recommended to develop and practice legislative norms that justify the right to digital evidence.

References

1. Istam Astanov, Bakhtiyor Khamidov. General theoretical issues related to electronic or digital evidence: problem and solution. Society and innovations. https://inscience.uz/index.php/socinov/index.
2. Karimov Boburjon. SCIENTIFIC AND THEORETICAL ISSUES OF THE CATEGORY OF DIGITAL EVIDENCE. Review of law sciences-Scientific-practical legal journal. Special issue. Part 5.
3. Karimov Boburjon. SCIENTIFIC AND THEORETICAL ISSUES OF THE CATEGORY OF DIGITAL EVIDENCE. Review of law sciences-Scientific-practical legal journal. Special issue. Part 5.
4. Goodison S.E., Davis R.C., Jackson B.A. Digital Evidence and U.S. Criminal Justice System // The National Institute of Justice, U.S. Department of Justice. – 2014. – P. 31
5. Зазулин.А.И. Использование цифровой информации в доказывании по уголовным делам: монография. М. Юрлитинформ, 2019. С. 55.
6. Ovie Carroll (Director US Department of Justice Cybercrime Lab Computer Crime & Intellectual Property Section). Challenges in Modern Digital Investigative Analysis .
7. The Final Chapter: Digital Forensics Served The Right Justice. https://fghani2.medium.com/welcome-back-to-our-blog-series-this-will-be-the-last-and-final-chapter-for-our-friend-steve-2b501780d64f.
8. Antwi-Boasiako and Venter, 2017; US National Institute of Justice, 2004.