GALAXY INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL (GIIRJ)
ISSN (E): 2347-6915
Vol. 13, Issue 5 May (2025)

DIGITAL EVIDENCE IN THE DETECTION AND INVESTIGATION OF CRIMES COMMITTED USING INFORMATION AND DIGITAL TECHNOLOGIES AND ARTIFICIAL INTELLIGENCE

Alimjan A. Matchanov,
Doctor of Law, Professor, Colonel Head of the Faculty for Work with Foreign Personnel of the Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan, 100146, Tashkent, st. Mumtoz, 4-way, building 6 E.mail: alimjan.matchanov@gmail.com Scientific specialty: 12.00.09 - Criminal trial. Criminalistics, operational-search law and forensic expertise UDC 343.985.7 ORCID 0000-0003-0670-8643

ABSTRACT

The article examines the concept, content and features of the algorithm for detecting, recording and using digital evidence in solving and investigating crimes committed using information and digital technologies and artificial intelligence. The stages of this algorithm are analyzed, tactical methods for detecting, recording digital evidence during inspection and subsequent seizure and assignment of computer-technical, software-technical and other types of examinations aimed at analyzing digital evidence are shown. Based on the opinions of domestic and foreign scientists, the author proposes solutions for improving the mechanism for using the capabilities of information and communication technologies and artificial intelligence in investigating crimes committed in virtual cyberspace.

Keywords: Digital evidence, information and digital technologies, crime investigation, artificial intelligence, stages of digitalization, algorithm of stages of detection of digital evidence.

INTRODUCTION

Information digital technologies (hereinafter referred to as ICT) and artificial intelligence (hereinafter referred to as AI) used on their basis are intensively developing in the world, and the legal and applied components of their growth are platforms for digital services of ICT and AI. At the same time, the recent increase in cases of theft using ICT and AI capabilities indicates the lack of "digital financial literacy of the population and the qualifications of law enforcement officers, the lack of modern systems for preventing such offenses[1].

Crimes committed using the capabilities of ICT and AI are international (transnational) in nature and, according to experts, the possible damage in this area in the world by 2030 may reach a record 90 trillion. US dollars[2].

Indeed, the development of the modern world, where there is a widespread introduction of ICT and AI, have made our lives dependent on them. But along with the positive aspects, the use of ICT and AI has made it possible to commit crimes in the information space through computer and other technical means used on the Internet and in other social networks. At the same time, the detection and investigation of crimes committed in virtual cyberspace requires both technical and legal knowledge. The emerging opportunities for illegal penetration into the virtual information network for the purpose of criminal enrichment of "cybercrime" (the

word "cyber" comes from the Greek, where "cybernetics" refers to the science of managing and transmitting information among people and machines).

This refers to the scientific terminology used in the investigation of crimes committed with the help of ICT and AI. In modern jurisprudence, such crimes are designated under various concepts and terms. The most common of them are: cybercrime; crimes committed using information and digital technologies; computer crime; digital, electronic crimes, etc.

The main means of solving and investigating crimes committed in the field of information technology is digital evidence, which has its own characteristics in comparison with traditional types of evidence. In a general sense, evidence in criminal proceedings is any factual data on the basis of which the investigating and court authorities establish the presence or absence of a socially dangerous act in accordance with the procedure established by law, the guilt of the person who committed this act, and other circumstances that are important for the correct resolution of a criminal case[3, p.69].

However, when it comes to crimes committed in the field of information technology, the specificity lies in the digital nature of evidence. This evidence can exist in various forms and requires special approaches to its detection, recording, seizure, examination and evaluation.

One form is computer data (files, documents, emails, databases, images, audio and video recordings, browser history, and other data stored on hard drives, servers, flash drives, and other storage media).

Another form is network traffic, which is implemented through connections between computers, IP addresses, connection times, and transmitted data.

Another form of digital evidence is log files, which record events that occur in operating systems, applications, servers, and network equipment, recording user actions, errors, access attempts, and other important events.

The next type of digital evidence is metadata, which is expressed in information about the data, such as the date and time of creation, author, file size, geolocation (for photos and videos), which may contain important evidence[4, p. 48].

Digital traces play an important role in the definition of digital evidence. They are expressed in the user's actions on the Internet, such as visiting websites, posting on social networks, online transactions, IP addresses of devices used to commit criminal acts.

To determine the features of digital evidence, it is necessary to know about the software used and the viruses available. The programs used to commit the crime, as well as viruses, Trojans and other malicious programs, can be evidence.

A body investigating crimes committed in the field of or through information (computer) technologies must have certain skills in working with digital evidence. In doing so, they must take into account their variability and fragility. Digital data can be easily altered, deleted, or destroyed, requiring a quick and skilled response when it is detected and captured. At the same time, according to D.V. Bakhteev, "doubts about the reliability of this or that evidence can manifest themselves in two main forms: in the source of evidence and in the correlation of evidence with each other" [5, p.18].

Digital evidence can be vast amounts of information, making it difficult to analyze and find relevant data. They also have a cross-border nature, which means that IT crimes are often

committed using infrastructure located in different countries, which makes it difficult to obtain and use evidence.

Working with digital evidence requires special knowledge and skills in the field of information technology, digital forensics and criminal procedure rules [6, p.52]. Therefore, it is necessary to comply with the procedural rules, procedures for the discovery, recording, seizure and examination of digital evidence, which must strictly comply with the law to ensure its admissibility in court.

The procedural algorithm for the disclosure and investigation of crimes has its own stages, which, from the point of view of criminalistic tactics of proof, were considered by us back in 2001 [7, p.63]. Currently, the content of the stages of the proof algorithm needs to be adjusted taking into account the development of digital technologies and the use of artificial intelligence.

The use of ICT and AI in the use of digital evidence in the detection and investigation of crimes in the field of information technology is a promising direction. The content of the algorithm for their application using ICT and AI can be implemented through the implementation of the following stages:

The first stage is the collection and pre-processing of digital evidence. The use of specialized software based on ICT and AI to automatically collect digital evidence from various sources (computers, networks, cloud storage, mobile devices, etc.) in compliance with legal procedures. The use of ICT and AI to filter duplicate and irrelevant data at the early stages. standardization of formats for various types of digital evidence (logs, event logs, memory dumps, network traffic, etc.). It is necessary to pay attention to the use of natural language processing (NLP) methods to extract structured information from text data (emails, messages in instant messengers).

The second stage of the algorithm for the use of ICT and AI in the detection and investigation of crimes committed in the field of information technology is the analysis and identification of patterns in the detection and recording of digital evidence.

At this stage, information and digital learning algorithms are used, which is based on cluster analysis to identify unusual activity in network traffic, log files or user behavior indicating criminal activity. Graph neural networks (GNNs) are used to analyze the relationships between various digital objects (users, IP addresses, files, domains) and identify hidden connections that may be important for the investigation. Classification algorithms (e.g., Support Vector Machines, Random Forests, neural networks) can be used to automatically categorize files, emails, messages by their content or characteristics (e.g., phishing emails, malware).

Information and digital learning methods are used to identify repetitive patterns in the actions of criminals, their tools and methods of committing crimes based on the analysis of previously investigated cases and current evidence.

The third stage of the algorithm under consideration is the interpretation of the results, the formation of an evidence base on which the visualization of the results of the analysis is carried out. This means the use of data visualization tools based on ICT and AI to present complex analysis results in an understandable form (graphs, diagrams, networks of connections), which facilitates their interpretation by the investigative authorities and the prosecutor's office.

conclusions, which increases confidence in the results of the analysis and allows you to substantiate them in court. Generation of reports, explanations in natural language, describing the identified patterns and relationships, as well as the use of ICT and AI. This is necessary for the automatic formation of probable hypotheses about the development of the crime and possible scenarios based on the analysis of evidence.

The fourth stage of the algorithm is expressed in supporting decision-making and presenting digital evidence obtained through forecasting and recommendations. Use ICT and AI to predict potential areas for further investigation and provide recommendations to investigators on next steps.

This algorithm is a general framework, and the specific steps and technologies used may vary depending on the type of crime, the data available, and the capabilities of law enforcement. However, the use of ICT and AI can certainly significantly increase the efficiency of working with digital evidence and speed up the process of solving and investigating the types of crimes in question.

To do this, it is necessary to know the peculiarities of the tactics of such investigative actions as the inspection of computer equipment, servers and other data carriers, as well as the seizure of the necessary data in compliance with the procedures established by law[8, p. 24].

Another important investigative action is the appointment and conduct of computer, hardware, software and other types of examinations aimed at analyzing digital evidence, restoring deleted data, establishing a sequence of actions and obtaining other important information stored in virtual space.

In the detection and investigation of crimes committed using information technology, it is necessary to ensure the safety of digital evidence. This also applies to the features of disclosure and investigation of cybercrimes[9, pp. 77-78]. To this end, measures should be taken to prevent unauthorized access, alteration or destruction of digital evidence.

Thus, the concept of evidence in the investigation of crimes committed using information technologies includes a wide range of digital data that require special attention to their collection, recording and analysis using specialized knowledge and compliance with procedural rules. Effective investigation of such crimes largely depends on the ability of the investigating authorities to work with these specific types of evidence.

The inevitability of criminal liability for such crimes, according to A.U. Rasulev, depends on increasing the effectiveness of the fight against crimes in the field of information technology. At the same time, he singles out such a priority area as ensuring the principle of inevitability of responsibility [10, p.37], which are based on the reliability of evidence.

N.A. Nugmanov, in turn, among the problems associated with the use of information technologies, will single out the creation of legal conditions for an electronic document as evidence [11, p.42].

In the disclosure and investigation of crimes, a special place is given to tactical methods of obtaining evidence through information technologies, which have created the prerequisites for the emergence of such specific forms as digital or electronic evidence.

In this regard, E.S. Ermakova notes that "electronic evidence is easily subject to change and instant destruction. At the same time, he highlights the following features of recording

electronic evidence: 1) Efficiency; 2) Participation of a specialist; 3) Availability of special devices for their recording, storage and reproduction" [12, pp. 85-87].

In our opinion, these features in the disclosure and investigation of crimes committed with the use of information technologies most fully reflect the criminalistic tactics of their acquisition. At the same time, it should be remembered about the features inherent only in this source of evidence, namely the fact of the formation of digital signals in virtual space.

The experience of solving and investigating crimes committed using information technology in the United States shows that in order to obtain digital evidence, special technical groups were created to study them – the Technical Working Group on Digital Evidence (TWGDE), which were later transformed into a single Scientific Working Group on Digital Evidence (SWGDE) [13].

According to N.A. Ivanov, digital evidence is understood as factual information obtained with the help of information and communication technologies of discrete signals contained or recorded on computer or other computer media, seized, transferred by the participants in the process or otherwise obtained in accordance with the current criminal procedure legislation [14, pp. 77-78].

One of the main tactical techniques for detecting, collecting and recording digital evidence in the disclosure and investigation of crimes committed using information technology is the seizure of digital media during the inspection. In this regard, V.A. Meshcheryakov and V.V. Trukhachev noted that "the arsenal of available procedural actions is quite large, it is nevertheless, on the one hand, limited to an exhaustive list, and on the other hand, for the purposes under consideration, it is actually reduced to one single investigative action – inspection" [15, pp. 108-110].

This is due to the fact that inspection is a universal investigative action, in which the perception of digital information provides for the presence of certain technical means and the necessary software that allows you to understand the essence of information expressed in digital form.

The authorities responsible for investigating crimes do not always deal directly with physical digital media. The peculiarity of information and telecommunication systems is expressed in the ability to obtain the relevant digital evidence that is important in the methodology of investigation, without having physical access to the location of the information carrier. At the same time, digital information is recorded in the inspection protocol drawn up using open sources available to users, but only when the data are placed on publicly available machine, computer or other information carriers [16, p.171].

Tactical methods of conducting this investigative action are expressed in direct penetration into the room where their machine, electronic and other information carriers are located. At the same time, the above type of evidence can be recorded on any material carrier, including those obtained as a result of the application and use of information and telecommunication technologies. In fact, they materialize as material evidence or an electronic document by means of which information presented in the form of digital signals is a material, computer (electronic) carrier, regardless of the means of their storage, processing and transmission. These can be hardware and software of microprocessor technology. At the same time, the evidence base consists of information recorded on computer media or on CDs, DVDs, flash

drives (portable media), as well as microprocessor, computer or other innovative equipment built into the means.

Thus, based on the above, it can be concluded that tactical methods of detecting and fixing digital evidence in the disclosure and investigation of crimes committed using digital technologies is a complex algorithm. It includes sequential actions that combine a set of activities related to forensic techniques and tactics for detecting, obtaining, and evaluating this digital evidence. Knowledge and ability to apply in practice the optimal forensic tactics of working with digital evidence will create the most effective and optimal methodology for investigating crimes committed using information technology.

REFERENCES

1. Decree of the President of the Republic of Uzbekistan No 381 of November 30, 2023 "On measures to strengthen the protection of the rights of consumers of digital products (services) and the fight against offenses committed by means of digital technologies" // National Database of Legislation, 30.11.2023, https://lex.uz/ru/docs/6681115.
2. См.: https://www.vedomosti.ru/importsubstitution/new_technologies/ articles/ 2023/03/14/966290-internet-neset-poteri (дата обращения 29.09.2024 года)
3. Razhabov B.A. Ensuring Compliance with General Conditions of Evidence in Pre-Trial Proceedings: Avtoref. dis. … Dr. Jurid. (DSc). – T., 2019. – 69 p.
4. Yangiev G.A. Improvement of the Institute of Evidence Assessment in Criminal Proceedings. dis. … Doctor of Philosophy (PhD). – T., 2021. – 48 p.
5. Bakhteev D. V. Kontseptual'nye osnovy teorii kriminalisticheskogo myshleniya i ispol'zovaniya sistem iskusstvennogo intellekta v rassledovanii prestuplenii [Conceptual foundations of the theory of forensic thinking and the use of artificial intelligence systems in the investigation of crimes]. dis. ... Dr. Jurid. Sciences. – Yekaterinburg, 2022. – P.18. (42 p.)
6. Oripov S.S. Improving the Use of Information Technologies at the Stage of Pre-Trial Proceedings: Avtoref. dis. … Doctor of Philosophy (PhD). – T., 2023. – 52 p.
7. Matchanov A.A. Problems of the Theory of Evidence in the Criminal Process: Monograph. – T.: Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan. 2001 – P. 63 (154 p.)
8. Ruzmetov B.Kh. Vyemka i poisk na predvaritel'nom sledstvii: sostoyaniya, tendentsii i perspektivy [Seizure and search at the preliminary investigation: state, trends and prospects]. dis. … Cand. jurid. Sciences. – T., 2008. – 24 p.
9. Matchanov A.A. Features of Disclosure and Investigation of Cybercrimes. Monograph – T. Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan, 2024. – 153 p.
10. Rasulev A.U. Improvement of Criminal Law and Forensic Measures to Combat Crimes in the Field of Information Technologies and Security. dis. … Dr. Jurid. (DSc). – T., 2018. – 74 p. (P.37)
11. Nugmanov N. A. Teoretiko-prakticheskо-prakticheskoe osobennosti formirovaniya mezhdunarodnogo informatsionnoy prava [Theoretical and practical features of the formation of international information law]. dis. … dock. jurid. (DSc). – T., 2018. – 59 p. (P.42)

12. Ermakova E. S., Dzhumangalieva D. M. Elektronnye dokazaniya kak novoye napravleniya v praktike rassledovaniia prestupleniy [Electronic evidence as a new direction in the practice of crime investigation]. – Text : immediate // Young scientist. – 2018. - № 23 (209). – P. 85-87. Available at: https://moluch.ru/archive/209/51196/ (accessed: 05.10.2021).
13. http ://ncfs.org/swgde/
14. Ivanov N.A. On the Concept of "Digital Evidence" // Bulletin of the Omsk Law Institute, 2006, No 2 (5), - P. 77-78
15. Meshcheryakov V.A., Trukhachev V.V. Formation of Evidence on the Basis of Electronic Digital Information // Bulletin of the Voronezh Institute of the Ministry of Internal Affairs of Russia. 2012. №2. – P.108-110.
16. Kartashov I.I. Non-Traditional Sources of Operational Information // Actual Problems of the Activities of Penal Correction Systems: Collection of Materials of the Open Scientific and Practical Conference / Voronezh Institute of the Federal Penitentiary Service of Russia. – Voronezh: Scientific Book, 2010. – P. 169 – 174. P. 171.