International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Digital Forensics in Modern Society: Exploring Investigations of Computer Crimes in the Context of the Russian Federations Criminal Code

Dr. S. Rajalakshmi

Head of the Department & Associate Professor, Department of Criminal Law and Criminal Justice Administration, School of Excellence in Law, The Tamil Nadu Dr Ambedkar Law University, Chennai - 600 113

Abstract

In this work, the authors raise the issue of the need to use and improve digital forensics methods in the investigation of various types of computer crimes. The goals and features of digital forensics are considered, as well as special operational-search activities are identified that are related to the specifics technical equipment and are necessary when investigating computer crimes. Almost every science has developed its own understanding of information and studied its various forms and aspects. In the 20th century, a new type of information appeared - information circulating in computers, and subsequently, in other information technology devices. However despite the fact that more than 7 decades have passed since the appearance of the first computer (we believe that the first computer can be considered the British Colossus, launched in 1943), and from the theoretical justification of developments in the field of computers and computer information even more time (the theory was laid down by Charles Babbage in 1830), even a generally accepted term that reflects the essence of this information, as well as a universal approach to the interpretation of the category under consideration. The life of modern society is difficult to imagine without the use of computer equipment, smartphones, tablets, as well as provided such devices for accessing the virtual space of the Internet, social networks, online stores, services provided remotely. However, all the advantages and advantages of the era of widespread digitalization are accompanied by the emergence of criminal activity in this new environment of human existence. This, in turn, causes the need for active research into its specifics and use of the results obtained in law enforcement. Recently it has become quite firmly established and developed as a relatively independent, but organically closely related, based and inseparable from the science of criminology, a direction called digital forensics.

Keywords: digital forensics, computerization, digital traces, computer technology, digital crimes

Introduction

Judicial and investigative practice shows that criminals use digital technologies and digital information when committing crimes. This applies not only to technical means used for interaction between members of a criminal group, but also to the possibility of distributing information prohibited by law

through information and telecommunication networks, for example, Art. 207 of the Criminal Code of the Russian Federation (Knowingly false report of an act of terrorism), Article 110.1 of the Criminal Code of the Russian Federation (Inducement to commit suicide or assisted suicide suicide), art. 242.1 of the Criminal Code of the Russian Federation (Manufacture and circulation of materials or items with pornographic images of minors), etc. Computer hardware is widely used in committing crimes in the field of economy, illegal drug trafficking and other crimes. To achieve forensic purposes, in our opinion, relevant digital information can be used in various forms, namely, as information, as operational (search) and as evidential. The purpose of this work is to study trace formation mechanism in digital environment of modern cybernetic space (information infrastructure) and the peculiarities of the formation of based on forensic evidence.

Material and research methods

The research is based on the general scientific dialectical method of cognition objective reality, as well as on special research methods. Validity of conclusions and recommendations, contained in the work is achieved through complex application of dialectical, analytical, logical, historical, system-structural, comparative legal, legal and linguistic methods.

Research results and their discussion

Today, one of the strategic directions for the implementation of state policy is the scientific and technological development of the Russian Federation. Information and telecommunication technologies are actively being introduced into all spheres of civil life society (social, managerial, healthcare, law enforcement etc.). At the same time, according to the General Prosecutor's Office of the Russian Federation, in 2019, there was an increase in crimes committed using the Internet, from 65.9 thousand (in 2018) to 91.6 thousand. It should be noted that the legal regulation of this sphere of life society often does not meet its needs development. A striking example is block chain technology, which is a system-forming link in the circulation of cryptocurrency. There is no legal definition of this payment document. At the same time the possibilities of its circulation in virtual space are unlimited. This is due to growth of mechanisms of criminal activity in this direction, where the cryptocurrency is may be a means of accomplishing crime, and the subject of a criminal attack. In this case you should talk about the formation of computer criminology as a branch of knowledge, skills and abilities aimed at developing competencies in identifying, solving and investigating crimes in the field information and telecommunications technologies, forensic research of electronic evidence information [1, p. 530].

Crimes of this category are committed in a non-contact manner, which significantly reduces the possibility of identifying trace traces and together thereby increasing the number of digital traces. In this article, a digital footprint is understood as a unique set of actions performed in the information and telecommunications environment, as well as information left as a result of browsing web pages. A digital footprint can be left as both an individual and a legal entity.

The prerequisites for the emergence of digital forensics were:

1. Emergence and active development cybernetic space (information infrastructure) as a new specific environment of existence and active activity of modern man with fundamentally new system-

forming elements. These elements are computers, computer networks (primarily the Internet), mobile telecommunication systems, global navigation systems, internet economy, etc.

2. Formation of fundamentally new types of legal relations that develop around objects and phenomena in cybernetic space that have no analogues in the traditional material world. In particular, we are talking about Internet sites, the domain name system, computer programs (especially self-reproducing ones, known as computer viruses), distributed systems registries (Blockchain), which became the basis for building a whole range of cryptocurrencies, social networks, unmanned transport platforms, etc.
3. The emergence of new types of attacks on emerging legal relations in cyberspace. For example, the use of malicious programs, mirroring and substitution of Internet resources, interception of real and generation of fictitious (intentionally distorted) information, etc.
4. Expanding the understanding of the mechanism of trace formation by supplementing it laws of cybernetic space, namely: electronic-digital display, virtual traces, new properties of emerging traces, features formation of a trace pattern, etc.

Law enforcement agencies for forensic purposes carry out accumulation, processing, systematization, storage and issuance of reference and accounting information, including digital. So, for example, police authorities maintain video banks and video libraries of persons who have undergone (are undergoing) cases and materials of police checks; form, lead and use operational reference data banks, forensic, forensic, investigative and other information about persons, objects and facts. Also a variety of integration software is used to expand the technical facilities. These include the facial recognition program “Find Face”. CCTV cameras, which will be this program is connected, they will be able to conduct analysis in real time resulting images and thus identify offenders [2, p. 231].

Level of development of digital technologies allows us to approach the implementation of such projects like Smart City. This is a complex software and technical solutions and organizational measures aimed at for the effective use of all types resources (electricity, water, gas, heat, time) and creating conditions for convenient stay in the city, comfortable for living and doing business [3, p. 16]. Such computerization of the city allows use technologies so-called “Intelligence devices” for collecting and analysing data about the behaviour of the subject, the routes of his movement and the persons with whom he makes contact. Example of use there may be similar devices in Amsterdam. To achieve the goals of operational investigative activities (ORA), many technical means have been developed that allow secretly receive information when carrying out this activity. Scroll special technical means used by bodies carrying out operational investigations, given in the Government Decree.

Without the use of digital technologies it would be impossible to obtain such information due to its specificity. Modern criminology must adapt to the level of development of modern technologies in order to be able to use them to provide assistance in law enforcement activities.

Nowadays, the term “Digital Forensics” has become frequently mentioned. This is due, firstly, to the fact that committing crimes using digital devices leaves electronic forensically significant traces, and secondly, with the fact that the preliminary authorities investigations have technical and forensic tools (personal computers) that allow the preparation of procedural documents in electronic form on electronic

media. This is also reflected in the norms of the Code of Criminal Procedure of the Russian Federation. Articles 164, 189 of the Code of Criminal Procedure of the Russian Federation and others allow the ability to record traces of a crime and the progress of investigative actions using technical means.

Cybercrimes often involve direct attacks on computers and other similar devices in order to shutdowns. Sometimes attacked computers used to distribute malware, illegal information, various types of images (for example, child pornography) and extremist materials. In the latest legal the literature identifies the following type's cybercrimes: selfish cybercrimes (including phishing, cyber extortion, financial fraud, etc.); identity theft; cyber espionage; cyberbullying; copyright infringement and some others. Considering them, it should be taken into account that in modern conditions, "non-traditional" species are actively entering into legal economic circulation property, including websites, cryptocurrencies, mobile communication technologies, Internet property, etc.

Because they have the ability generate high incomes, the criminal environment reacts to them accordingly. As a result, new types of criminal attacks appear, involving the use of modern information technology based surprise and anonymity.

Almost all of these illegal actions are much more dangerous than crimes, committed outside of cyberspace because they are capable of causing damage all legally protected interests. They range from private non-property the needs of individual citizens to the needs state security. An analysis of official crime statistics shows that amid the coronavirus pandemic, the overall crime rate in Russia remained the same, but the number of cybercrimes has increased sharply.

It's not only costs of digitalization of society, but also the result of the fact that people, being in self-isolation, have more opportunities to acquire various knowledge online, including criminally oriented, and apply them in practice.

This state of affairs has led to that in 2019 in the structure of one of the key departments of the Investigative Committee of the Russian Federation a new Division – Cybercrime and Crime Investigation Department in the field of high technology. Soon after this is a similar wrestling unit with IT crimes appeared in the Investigation Department of the Russian Ministry of Internal Affairs. Their the emergence is associated not only with pronounced specificity, widespread and high latency of cybercrimes, but also with their inherent interregional and international character. Ministry of Internal Affairs of the Russian Federation published statistics according to which 420,700 cybercrimes were reported in the first 10 months of 2020 (+75%), of which 216,000 are serious or especially severe (+84%).

The number of crimes using the Internet in the same year increased by 93% and amounted to 243,600 units, and using mobile communications - by 96% and reached 181,200 units. For the same period, the increase in the number of crimes using bank cards amounted to more than 480%. The leader in the growth of cybercrime during this period was St. Petersburg, where such criminal acts were committed 290.5% more than in the previous year. The Kaluga region is a little behind (207.3%), Karachay-Cherkessia (185.1%), Ingushetia (142.1%) and Samara region (119.9%). The lowest rates of their

growth are observed in Tyva (32.2%), Adygea (20%), Smolensk region (11.2%), Northern Ossetia-Alania (6.9%) and Kirov region (3.8%). At the same time the highest the level of detection of such crimes is observed in Dagestan. There is effectiveness in the fight against cybercriminals increased by 65%. Next come Karachay-Cherkessia (58.1%), Chechnya (58%), Chukotka (53%) and Ingushetia (42.6%). Lowest their disclosure rate in Bashkortostan (16.1%), Krasnodar Territory (15.7%), Tyva and Novosibirsk region (15.3%), as well as in the Tver region (14.5%). It should be noted that these statistics are very approximate. They should be treated with sufficient caution because The system for statistical recording of cybercrimes is still far from ideal due to the fact that that the procedure for officially declaring and confirming actual financial losses caused as a result their commission to Russian organizations, institutions, enterprises and citizens, is still in its formation stage.

Currently, due to the development information and telecommunications technologies that are actively being introduced into all spheres of human activity, increasingly began to identify specific traces that arise in an artificially created digital display environment based on computer systems.

An essential feature of this situation is that the real object or the process of the surrounding reality is perceived by the subject of criminal procedural research not directly, but through a formalized (mathematical) model with the help of which this real object is described. Since a person builds a formalized model based on his goals and objectives, then it naturally does not cover everything elements, properties and behaviour of real object, reflecting in detail only those of them that meet the needs of the creator artificial reflection environment.

Moreover, in material form (in the form numerical set) only the parameters of the formalized system used are recorded models. Almost all scientists who study the mechanism of trace formation in virtual space recognize its specificity and the difference in the resulting traces from all other types previously considered by forensic science. Together However, to clearly formulate how this difference is expressed and how to briefly call it all remains a question on which there are many different points of view. In the specialized literature these new traces are called binary, informational, computer, computer-technical, digital and electronic-digital (electronic) traces.

In our opinion, it is rational to call these traces virtual traces, since this concept is the most fully reflects the fact of using a formalized model for the artificial construction of all manifestations of interest to the creator of the artificial environment observed object or phenomenon. Circuit the formation of virtual traces seems to be the most difficult among other listed above, since it uses an artificial environment for displaying real objects and phenomena (built based on computer systems), as well as environment for interaction of computer systems [3, p. 31].

Perceptions emerging in the circuit virtual traces of information are carried out by the subject of criminal procedural research using decoding methods and interpretation of numerical data sets. The complex picture of the joint and interconnected formation of material, ideal and virtual traces forms a whole range of features of the trace formation mechanism, which create the basis for the subject of digital forensics.

Conclusion

Thus, electronic digital information can be defined as information recorded in any way, but transformable into human readable view using electromagnetic interactions and encoded using digital code, suitable for automatic processing, located in information technology devices and transmitted between them in any way or distributed between them. Except determining the range of information, delimiting the existing information technology objects under study from developments, which are in the distant future and require other research methods (and clearly to quantum, optical, biological and other promising areas of development of alternative devices will not apply the existing recommendations due to the specifics of their work, circulation of information and the range of tasks to be solved), the approach proposed here will allow comprehensively take into account the specifics of the object of theoretical research and unify investigative and judicial practice, eliminating errors and discrepancies associated with different approaches to differentiating electronic and digital devices [5, p. 124].

Bibliography

1. Smushkin A.B. Object and subject of electronic digital forensics // Technologies of the XXI century in jurisprudence: materials of the 2nd international. Scientific-practical conf. (Ekaterinburg, May 22, 2020) / ed. D.V. Bakhteeva. Ekaterinburg: Ural State Law University, 2020. pp. 530-541.
2. Obidin K.V. On the role of electronic information in criminal proceedings in the context of digitalization // Bulletin of the University named after O.E. Kutafina. 2020. No. 10 (74). pp. 231-236.
3. Belomytsev N.N. Cryptocurrency as a subject of theft through the use of computer equipment // Use of cryptocurrencies for illegal purposes and countermeasures: materials of the international. scientific-practical round table (Moscow, April 25, 2019) / under general. ed. A.M. Bagmeta. M.: Moskovskaya Academy of the Investigative Committee of the Russian Federation, 2019. pp. 16-22.
4. Pastukhov P.S. Information technology devices for electronic evidence / Fundamentals theories of electronic evidence: monograph / ed. Doctor of Law Sciences S.V. Zueva. M.: Yurlitinform, 2019. pp. 31-62.
5. Sukmanov V.O. Essence, concept and types of electronic digital traces used in solving and investigating crimes // Bulletin of the Kaliningrad Law Institute of the Ministry of Internal Affairs of Russia. 2020. No. 4 (22). pp. 124-127.