ATLANTIS PRESS
Advances in Economics, Business and Management Research, volume 110
5th International Conference on Economics, Management, Law and Education (EMLE 2019)

The Areas of Concern in Using Digital Technologies for Documenting Criminal Acts and Collecting Evidence at the Prejudicial Stage of Criminal Proceedings

Anatoly Vyacheslavovich Tarasov
Department of Criminal Procedure Law
North-Caucasus Branch of Russian University of Justice
Krasnodar, Russia
E-mail: tarasov-av@mail.ru

Alexander Ivanovich Gaevoy
Department of Criminal Procedure Law
North-Caucasus Branch of Russian University of Justice
Krasnodar, Russia

***Abstract*—The article focuses on the main problems of using digital technologies in crime investigation and analyses the digital opportunities for documenting the traces of crimes and adducting evidence in criminal proceedings.**

Keywords—digital technologies; Internet; traces of crimes; digital means of fixation; operational investigations; crime investigation

I. INTRODUCTION

The 21st century is the era of digital technology; therefore, all social processes taking place worldwide are inevitably linked with using computer environment. As stated in the Strategy for the information society development in the Russian Federation for 2017-2030, approved by the Presidential Decree, "information society is the society in which information, its application and accessibility have a significant impact on the economic and sociocultural conditions of people's lives". "In Russia, the information society is characterized by the widespread occurrence and accessibility of mobile devices (on average, there are two mobile telephony customer numbers per Russian citizen), as well as wireless technologies and communication networks" [1].

The established information environment of public relations has its new name - "cyberspace". However, this virtual world has built a climate for committing various crimes.

In Russian criminal legislation, there is a qualifying attribute "with the use of mass media, electronic or information and telecommunication networks (including the Internet)", which prescribes increased accountability for a number of criminal acts, for example, under articles 171.2, 205.2, 228.1, 242, 242.1, 242.2, 280, 280.1, 282 of the Criminal Code of the Russian Federation.

Computers, laptops, smartphones, smart TVs and many other gadgets have become an integral part of people's lives in modern world. According to E.P. Ischenko, the functioning of these devices and their interaction in the information transfer by means of telecommunication channels, contribute to the establishment of the information environment, "where specific traces of various human activities are reflected, recorded and stored" [2].

The interaction with electronic, information and telecommunication networks reflects the illegal behaviour and its individual manifestations in the actions of certain legal subjects, and provides what is commonly referred to as digital footprints of a crime (law violation).

An accurate definition of a "digital footprint" has been proposed by V.B. Vekhov. According to him, "a digital footprint is any forensically significant computer information, i.e. the information (messages, data) presented as electrical signals, regardless of the means of its storage, processing and transfer" [3].

At the current stage, preventing and solving crimes in "cyberspace" requires the application of the mechanism of marking formation to a variety of information systems and storage media, which leave digital footprints when working with files in different operating systems.

One of the critical stages in the algorithm of taking evidence in crime investigation is its documentation. D.V. Mulenkov described digital fixation as "the process of digital technology application by a specially authorized subject of criminal proceedings in the manner prescribed by law. It is aimed at objective, efficient, comprehensive and informative demonstration and consolidation of properties, qualities, forms of material objects, the process and results of ongoing operational investigation activities, investigative actions and legal proceedings in order to hold the factual data in the criminal case files or to use it as facts and circumstances relevant to the criminal case" [4].

Nowadays, digital technologies are gaining more and more popularity and are competing favourably with traditional means of audio, video and photographic fixation. Digital technology is becoming a regular working tool for

operations officers of various departments. Modern technical means of documentation have profound influence on improving the old and developing the new methods and tactics for detecting, documenting and examining the evidence in the process of solving and investigating crimes. Therefore, special attention to any changes in technology is fairly understandable: audio, video, photographic fixation tools make receiving, recording and processing evidentiary information when solving and investigating crimes much easier, faster, more economical and efficient.

Nevertheless, when legislative innovations, hypotheses and expectations are confronted by the real practice of investigating criminal cases, there appear a host of contradictions and problems for the officials involved in the mechanism of digital technologies application.

II. Using Digital Technologies in Operational Investigation Activities

Presently, when solving and investigating crimes, the major role in terms of using digital technologies for detecting, recording and investigating digital footprints of crime preparation or commission, is performed by the bodies, which carry out operational investigations, and the specialists in the field of latest forensic means application.

As stated in article 6, paragraph 4 of the Federal Law "On operational investigation activities", operational investigation activities related to 1) mail, telegraph and other messages cover, eavesdropping on telephone conversations with the connection to the permanent equipment of companies (regardless of their ownership), individuals and legal entities providing communication means and services; 2) information retrieval from communication channels; and 3) the receipt of computer information; are performed by means and operating forces of the Federal Security Service and internal affairs bodies.

The system of operational investigation activities in the field of digital technologies has been implemented in Russia since 2014. It is designed in order to store metadata, which is the information about calls, Internet sessions and sent messages, as well as to collect the data about the service receivers from the telecommunications operators' internal systems.

In May 2016, the State Duma Committee on Security and Anti-Corruption Enforcement recommended to pass in its first reading the anti-terror draft amendments prepared by the Chairman of the State Duma Committee on Security, Irina Yarovaya, and the Chairman of the Council of the Federation Committee on Defence and Security, Viktor Ozerov.

The document contained amendments to the Law "On Telecommunications", which obliged Russian telecommunications service providers to store data on citizens' voice and text messages. According to the accepted amendments, for the period of three years, telecommunications operators should store within the country all the information "on the reception, transfer, delivery and processing of voice and text messages, including their content, as well as images, sounds or other messages of communication services users". Operators are to "provide this information to authorized government bodies performing operational investigation activities or ensuring the security of the Russian Federation".

As a result of amendments to the Law "On operational investigation activities", a new operational investigation activity was introduced - the acquisition of computer information.

On July 1, 2018, the system of operational investigation activities provided for by Yarovaya Law was launched in the country. Since then, telecommunications service providers are to store the records of correspondence and calls, made or received by their users for the period up to six months, and the information about the facts of their communication, that is, metadata - for the period up to three years.

The regulations for telecommunications service providers on storing service users' text, voice messages, images, sounds, video, etc. were approved by the Government Resolution of the Russian Federation No. 445, dated April 12, 2018. The document established different regulations for the operators, who transfer both text and voice information, and those, who do not transfer voice information. The first group includes telecommunications service operators providing national and international telephony, private mobile radio, cellular mobile radio, mobile radiotelephone and communication-satellite service, data communication services for voice information transfer, in-zone telephone communication, and local telephone communication. As for the second group, it comprises telecommunications operators providing telematic communication services and/or communication services for data transfer, except for those aimed at transmitting voice information.

The bodies carrying out operational investigation activities have the right to eavesdrop on telephone conversations, obtain the information from communication channels and receive computer information only in compliance with a court order.

According to the judicial department of the Supreme Court of the Russian Federation, in 2016, general jurisdiction courts issued 893.1 thousand of such orders to operations bodies to eavesdrop on telephone conversations and monitor correspondence and records created via the Internet (messages in social networks, emails, messengers, etc.) [5].

The latest innovation in the legislation regulating the conduct of operational investigation activities was the amendments to the Federal Law No. 144-FZ "On operational investigation activities" approved by the Parliament in July 2019. Operations officers, tracing under-age missing persons got the right to "obtain the information on the connections of an under-age user's device with other users, their devices and other equipment, and the geolocation of the user's device through information readout from technical communication channels..." [6].

Thus, for the first time, by means of the statutory act, regulating the implementation of operational investigation activities, the legislative body enshrined in law the receipt of geographical metadata from telecommunications service providers.

When analysing the main provisions of the new legislation, a reasonable question of legalizing operational investigative digital information arises. How can computer information in the form of "voice information and text messages, their content, images, sounds, etc.", obtained in operational investigative activities, be applied in criminal law and procedure? The major task of this work is the integration of digital footprints (information) into the system of existing evidence in conformity with the form of action of evidence reception. It is one thing, if digital footprints are the result of operational investigative work, performed over a certain period of time; this practice is well-established and tested by law enforcement agencies. However, it is different, if the work is performed post factum (after a crime is committed) and is aimed at searching and collecting digital information to prove those who committed the crime guilty. Therefore, all the investigative work on solving crimes is retrospective in nature. For instance, let us take receiving important "voice information" through telephone communication, - what is the mechanism of its legalization?

As stated in the requirements of the Russian Federation Code of Criminal Procedure and the Law "On operational investigation activities", "voice information" (mobile communication records) documented and stored by telecommunications service providers without a judicial decision, does not constitute the result of operational investigation activities and cannot be submitted to the corresponding investigating body in the manner specified by the "Policy and procedure for providing the results of operational investigative activities to the interrogator, investigator or court", approved by an interdepartmental order dated September 27, 2013. Under article 89 of the Russian Federation Code of Criminal Procedure, if the results of operational investigation activities do not meet the requirements for evidence established by the legislation, they cannot be used. What is more, when performing operational investigation activities, operational officers happen to make serious mistakes in executing documents and documenting traces of crimes. Eventually, these mistakes make it impossible to use traces of crimes as evidence, and result in evidence loss or evidence inadmissibility. In such cases, this data is likely to remain operational-relevant information that will not be possible to legalize. The court practice currently being established will inevitably face this problem.

III. Jurisdictional and Tactical Basis for Using Digital Technologies in Solving and Investigating Crimes

The procedural order of applying information technology means of evidence collection to investigating crimes, which have been committed with the use of modern digital technologies, consists of a few investigative activities. They include the following: examination (articles 176-177 of the Russian Federation Code of Criminal Procedure); search (article 9.1, para. 182 of the Russian Federation Code of Criminal Procedure); seizure (article 3.1, para. 183 of the Russian Federation Code of Criminal Procedure); monitoring and recording conversations (article 186 of the Russian Federation Code of Criminal Procedure); collecting information on two-party connections and/or connections between user equipment (article 186.1 of the Russian Federation Code of Criminal Procedure); and commissioning and performing expert evidence (articles 195, 199, 204 of the Russian Federation Code of Criminal Procedure). Notably, the last three investigative actions are fully implemented through the use of technical means. The rest are limited to the process of detecting, documenting and seizing forensically significant digital storage media.

Thus, legal investigators and interrogators widely use digital equipment (laptops, tablets, smartphones, etc.). In addition to the traditional ways of using mobile phones to consolidate photo, audio and video information, there appear some new technical and digital opportunities of documenting investigative proceedings. In particular, using a smartphone with a GPS-module during investigative actions (checking the testimonial evidence on-site, crime re-enactment, and crime scene examination) allows to geolocate. What is more, if the goals and objectives of the procedure require participants moving or relocating during the investigative action, it records the tracking route, providing the cartographical information.

Due to photo geolocation (geotags in photographs), the actions of suspects (witnesses, victims, etc.) can subsequently be analysed. The new information sources can be identified, for instance, the information from external surveillance cameras, etc., which in the process of investigation may become a form of evidence (testimony of witnesses in contact with persons of interest to the investigating authorities).

Collecting information on two-party connections and/or connections between user equipment carried out under article 186.1 of the Russian Federation Code of Criminal Procedure, allows the investigator, in cooperation with operations officers, to track all calls made from the crime scene (i.e. billing - the analysis of the service receivers' network activity in the search radius), and identify the digital footprints recorded by network base stations.

However, identifying and collecting digital information (accompanied by technical procedures and the procedural order of storing information not only as individual data objects, but also on electronic media) and studying digital footprints require special knowledge.

The modern criminal procedure legislation documents two forms of specialists' participation: as an investigator's right or a responsibility. It means that the investigator has the right to call for a specialist to participate in some investigative proceedings, such as: examination (articles 176-177 of the Russian Federation Code of Criminal Procedure); crime re-enactment (article 181 of the Russian Federation Code of Criminal Procedure); arrestment of postal items, their inspection and seizure (article 185, para. 5 of the Russian Federation Code of Criminal Procedure). However, in case of search and seizure, under paragraph 9 ¼ article 182 and paragraph 3 ¼ article 183 of the Russian Federation Code of Criminal Procedure, it is a responsibility, so the investigator is obliged to call for a specialist to "seize electronic storage media".

Nowadays, the tactics, methods and tools of digital forensic science are actively used by the criminalists of the Investigative Committee of the Russian Federation, the Federal Security Service and the Ministry of Internal Affairs of the Russian Federation.

Investigative actions, related to the inspection and seizure of computers, mobile devices and digital media are carried out in cooperation with the employees of the Main Department of Forensics. In order to quickly detect the directory and evidentiary information on digital media, which can be used to solve the crime shortly after, the immediate inspection of the seized equipment is organized and carried out. The performed computer forensic analyses and video examinations allow to study the relevant digital information thoroughly [7].

In this respect, the statistics on the number of examinations of digital devices looks informative: in 2015, the forensic departments of the Investigative Committee of the Russian Federation carried out 2,062 examinations with 5,413 objects examined, whereas in 2016, 2,880 examinations were performed with 10,705 objects examined. It is worth mentioning that according to the statistics of the Investigative Committee of the Russian Federation, the number of computer devices examinations increased by 40%, whereas the number of examined devices grew by 98%.

In the conditions of the increasing volumes of seized media and the growing number of legal proceedings being performed, ensuring the availability of a specialist in each proceeding is becoming hugely problematic due to a number of objective reasons.

In this regard, some scientists' view on the problem of the legitimacy of seizing electronic data storage media without the participation of a specialist is of particular interest. According to them, "technically, the obstruction of the procedure of seizing electronic data storage media in most cases has no connection with infringing upon the rights and lawful interests of parties to the criminal process. Consequently, there are no grounds for declaring the investigative activities performance illegal, or for recognizing the seized electronic media as inadmissible evidence" [8].

This point of view is controversial, as it contradicts to the principle of evidence admissibility. Under article 75 of the Russian Federation Code of Criminal Procedure, the evidence, which has been obtained in breach of the statutory requirements of the Code of Criminal Procedure is considered inadmissible.

Nevertheless, we should acknowledge the imperfect requirements of paragraph 9.1, article 182 and paragraph 3.1, article 183 of the Russian Federation Code of Criminal Procedure, under which the participation of a specialist in the seizure of electronic storage media is obligatory. The legislative body making amendments to the Russian Federation Code of Criminal Procedure, was guided by the need for professional knowledge in digital technologies to be applied to investigative actions. In fact, this imperative leads to technical obstruction of the procedure of seizing electronic data storage media. From our perspective, it is essential to modify procedural legislation and to entitle the investigator to decide when to bring expertise.

Another important aspect of using digital footprints in the process of taking evidence in crime investigation is the preparation and conduct of forensic expert research.

According to the statistical data, in 2016, the expert departments of the Ministry of Internal Affairs of Russia carried out 21,792 computer examinations and research, which is 12% greater than in 2015. In 2016, the forensic departments of the Investigative Committee of the Russian Federation performed 1,323 computer forensic analyses, which represents an increase of 1% compared to 2015. A slight increase in the number of computer forensic analyses in the forensic departments of the Investigative Committee of the Russian Federation is not informative, as the figures need to be studied with respect to the number of objects under analysis: 3,234 objects in 2015 versus 4,307 objects in 2016 (33% growth).

The quality of expert research is directly related to the digital information submitted for examination. In this respect, there have developed two problematic trends: poor-quality copies of digital information (or obtained through violation of technical requirements) and edited digital records.

The falsification of digital footprints by using special software has become widespread, especially when it comes to audio files. The methodology for conducting phonoscopic examination provides the definition for an "indicator of editing" in an audio file. It is a change in a phonogram, which makes the audio information unreliable (due to distortion of the acoustic event or the content of the conversation, cutting or adding episodes, remarks, noise, etc.).

The development and wide dissemination of computer tools for processing and editing digital recordings alongside with the accessibility of detailed information on how these actions are performed, have made falsificating audio records or photos a simple thing to do even for non-professionals. That is exactly why enhancing the methods of assessing the adequacy and reliability of digital recordings is an essential scientific, technical and social task.

IV. CONCLUSION

Digital technologies are gradually spreading in various areas of people's lives, thus significantly accelerating information processing. They make audio, video and photographic evidence, as well as the opportunities of information exchange, more accessible. Digital technology is becoming a regular tool used by the bodies, which carry out investigative activities, legal investigators and interrogators. Modern technical means of documentation lead to improving the old and developing the new methods and tactics for detecting, documenting and examining the evidence in the process of solving and investigating crimes.

Numerous issues related to the integrated use of digital documentation as a way to make the process of adducting evidence in criminal investigations objective, as well as to

increase the effectiveness of investigative activity and the visibility of expert activities, require thorough study at the legislative, methodological and practical levels.

REFERENCES

[1] The Decree of the President of the Russian Federation No. 203, dated May 9, 2017 "On the strategy for the information society development in the Russian Federation for 2017-2030". // Available at: pravo.gov.ru.

[2] Ishchenko E.P. The current stage of Russian forensic science development // Forensic readings on Lake Baikal - 2015: the proceedings of the international research to practice conference, East-Siberian Branch Russian State University of Justice, 2015, p. 58.

[3] Vekhov V. B., Smagorinsky B. P., Kovalev S. A. Digital footprints in the forensic science system // Forensic enquiry, 2016, No. 2 (46), p. 17.

[4] Mulenkov D.V. Using digital means of documenting at the stages of pre-trial procedure: author's abstract for PhD in Juridical sciences. Tyumen, 2008. Available at: https://www.dissercat.com/content/ispolzovanie-tsifrovykh-sredstv-fiksatsii-na-stadiyakh-dosudebnogo-proizvodstva

[5] https://www.rbc.ru/newspaper/2017/11/09/5a03187e9a7947d88f988f53

[6] Federal Law No. 144-FZ, dated 12 August, 1995 "On operational investigation activities" (edited 2, August, 2019) // Consultant Plus.

[7] Yakovlev A.N. Digital forensic science and its importance in crime investigation in modern information society. // Improving investigative activities in the context of informatization: the proceedings of the international research to practice conference (Minsk, April 12-13, 2018) / Investigative Committee of the Republic of Belarus; editorship: S.Ya. Azemsha [et al.]. - Minsk: Editorial office of the journal "Industrial and Commercial Law", 2018, 368 p. ISBN 978-985-6789-34-5. Pp. 357-362.

[8] Kozlovsky P.V., Sedelnikov P.V. A specialist's participation in the seizure of electronic media // Scientific Bulletin of the Omsk Academy of the Ministry of Internal Affairs of Russia, 2014, No. 1 (52), p. 18.