Investigation and Seizure of Electronic Media in the Production of Investigative Actions

Submitted: 8 July 2019
Revised: 6 August 2019
Accepted: 25 January 2021

Article submitted to peer blind review

Vitalii Fedorovich Vasyukov*
ORCID: https://orcid.org/0000-0003-0743-5616
Zarina Ilduzovna Khisamova**
ORCID: https://orcid.org/0000-0003-0561-8718

DOI: https://doi.org/10.26512/lstr.v13i2.25920

Abstract

[Purpose] This article is devoted to the study of the problem of authorization of the removal of electronic media according to Russian Criminal Procedure Code.

[Methodology] The methodological basis of this study is a set of methods of scientific knowledge, among which the main place is taken by the methods of historicism, consistency, analysis and comparative law. The authors' position is based on the legislation and opinions of the competent scientific environment on the need to use special knowledge in the investigation and seizure (copying) of electronic information relevant to the criminal case.

[Findings] Based on a legal analysis of the rules of criminal procedure authors argue the necessity to use specialists in the field of information and communication technologies in inspections, searches, and seizures. The systematization of rules-exceptions that must be observed by investigators during inspections, searches, and seizures is carried out. The questions of the evidentiary value of the results of electronic withdrawal are raised.

Keywords: Electronic Media. Seizure. Criminal Activity. Electronic Devices. Investigation.

*Vasyukov is a well-known Russian forensic scientist, is an associate professor of the Department of Criminal Law, Criminal Procedure and Forensic Science of the MGIMO of the Ministry of Foreign Affairs of Russia, Doctor of Legal Sciences. In 2010 he defended his dissertation for the PhD. In 2018 he received the degree of Doctor of Legal Sciences. Present research interests include the problems of qualification, detection and investigation of crimes in the field of information and communication technologies. He is the author of more than 90 scientific, educational and methodical works. E-mail: vvf0109@yandex.ru.

**Khisamova is the head of scientific department of Krasnodar University of the Ministry of Interior of Russia. In 2016, she successfully defended her PhD thesis. She is a participant of international research conferences and forums, constantly reports her scientific developments and posts her articles in lead world publications. Her research interests include studying the problems of criminal law counteraction to IT crimes committed in the financial sector, criminal law protection of relations in the digital economy, and creating a regulatory environment for the introduction of new digital innovative products. She is the author of more than 50 scientific and educational works and is actively engaged in expert activities. E-mail: alise89@inbox.ru.

INTRODUCTION

The growth of computer-related crimes is observed all over the world. This is also true for the Russian Federation. So, in 2013, 10942 crimes were registered in this area, in 2014 - 10968, in 2015 – 43816, in 2016 – 65949, in 2017 - 90587 crimes. In 2018, more than 130 thousand such crimes were already registered. This situation has become a driving force for the increased need for specialized knowledge in the field of information technology (Kolycheva, 2019).

A.I. Bastrykin, the Chairman of the Investigative Committee of the Russian Federation, stressed that "...during the first half of 2018, forensic investigators took part in the inspection of almost two thousand electronic devices. Among the inspected objects - computers, laptops, tablets, mobile phones, removable media..." (Investigative Committee of the Russian Federation, 2018).

The procedure for involving a specialist in a criminal case is regulated by article 58 of the Code of Criminal Procedure.

> The art. 58 of the Code of criminal procedure "Specialist"
>
> 1. Specialist - the person possessing special knowledge and invited to participate in the proceedings in the manner prescribed by the Criminal procedure Code, to assist in the discovery, securing and seizure of items and documents, use of technical means in the study of the materials of the criminal case, to pose questions to the expert and to explain to the parties and the court on matters within his professional competence.
> 2. Calling a specialist and the procedure for his participation in investigative and other procedural actions, court sessions are determined by Articles 168 and 270 of this Code.
> 2.1. The defense party may not be denied a request to involve a specialist in the criminal proceedings to clarify issues within its professional competence, except for the cases provided for in Article 71 of this Code. (*A specialist has no right to take part in the proceedings in a criminal case if he is a victim, a civil plaintiff, a civil defendant or a witness in this criminal case; participated as a juror, expert, specialist, translator, interpreter, assistant judge, secretary of the court session, defense lawyer, legal representative of the suspect, accused, representative of the victim, civil plaintiff or civil defendant, and the judge also-as an inquirer, investigator, prosecutor in the proceedings on this criminal case; is a close relative or relative of any of the participants in the proceedings in this criminal case, have other circumstances that give reason to believe that they are personally, directly or indirectly, interested in the outcome of this criminal case; the specialist was or is in official or other dependence on the parties or their representatives; his incompetence will be revealed).*
> 3. The specialist has the right to:

> 1) refuse to participate in the proceedings in a criminal case, if he does not have the relevant special knowledge;
> 2) ask questions to the participants of the investigative action with the permission of the inquirer, the investigator and the court;
> 3) get acquainted with the protocol of the investigative action in which he participated, and make statements and comments that are subject to entry in the protocol;
> 4) bring complaints against the actions (inaction) and decisions of the inquirer, the head of the inquiry unit, the head of the inquiry body, the inquiry body, the investigator, the prosecutor and the court that restrict his rights.
> 4. Specialist is not entitled to evade the attendance at the summons of the inquirer, investigator or the court, as well as to divulge data of the preliminary investigation, which became known to him in connection with participation in the criminal proceedings as a specialist, if he was warned about it in advance in the manner prescribed by article 161 of this Code. The specialist is responsible for the disclosure of the preliminary investigation data in accordance with Article 310 of the Criminal Code of the Russian Federation.

The general conditions for the conduct of investigative actions are set out in art. 164 of the Code of Criminal Procedure. As a general rule, the production of investigative actions is authorized by the investigator. Individual investigative actions are carried out with the permission of the court. The specifics of removing electronic data carriers and copying information from them during investigative actions are defined in Art. 164.1 of the Code of Criminal Procedure of the Russian Federation. Part 4.1 of Art. 164 of the Criminal Procedure Code of the Russian Federation was added relatively recently.

According to the specified norm, when conducting investigative actions in criminal cases on crimes committed in the field of entrepreneurial activity, the unjustified seizure of electronic information carriers is not allowed. At the same time, the legislator designated the cases provided for in Part 1 of Art. 164.1 of the Criminal Procedure Code of the Russian Federation as exceptions to this rule.

> The art. 164.1. of the Code of criminal procedure "Peculiarities of withdrawal of electronic media and copy them in the production of investigative actions"
>
> 1. In criminal proceedings on business activity, the seizure of electronic data carriers is not allowed, except in cases where:
> 1) a decision on the appointment of a forensic examination in respect of electronic media has been issued;
> 2) the seizure of electronic data carriers is carried out on the basis of a court decision;
> 3) electronic data carriers contain information that the owner of the electronic data carrier does not have the authority to store and use, or that can be used to commit new crimes, or the copying of which, according to a specialist, may entail its loss or change.

> 2. Electronic data carriers are seized in the course of investigative actions with the participation of a specialist. At the request of the legal owner of the seized electronic media or the owner of the information contained therein, the specialist involved in the investigative action, in the presence of witnesses, copies the information from the seized electronic media. The information is copied to other electronic media provided by the legal owner of the seized electronic media or the owner of the information contained therein. Copying of information is not carried out in the presence of the circumstances specified in paragraph 3 of part one of this Article. Electronic data carriers containing copied information are transferred to the legal owner of the seized electronic data carriers or to the owner of the information contained on them. On the implementation of copying information and on the transfer of electronic media containing copied information to the legal owner of the seized electronic media or the owner of the information contained therein, an entry is made in the protocol of the investigative action.
> 3. The investigator in the course of the investigative action has the right to copy the information contained on the electronic data carrier. The protocol of the investigative action must indicate the technical means used in the process of copying information, the procedure for their use, the electronic media to which these means were applied, and the results obtained. The protocol shall be accompanied by electronic data carriers containing information copied from other electronic data carriers during the course of the investigative action.

The adopted amendments to the Russian criminal procedure legislation are quite timely and logical. Analysis of foreign legislation has shown that such norms are already contained in procedural torts.

Thus, in accordance with Article 39 bis of the Belgian Code of Criminal Procedure, if necessary, information is found in a computer network, it can be copied to an electronic data carrier without removing the electronic device containing the information.

In this case, the prosecutor ensures the safety of the seized data by using the necessary technical means. If the data is the object of a crime; obtained by criminal means; contradicts the recognized principles of morality or public order; or it poses a threat to the security of other data stored in a computer network, the court must take measures to ensure the inaccessibility of such data. If it is impossible to copy the necessary data, the prosecutor is obliged to ensure their safety and the inability of third parties to access them (Criminal procedure code of Belgium, 2018).

PROCEDURAL EXCEPTIONS TO AN ELECTRONIC EXEMPTION

The first exception for the law enforcement officer is cases when a decision on the appointment of a forensic examination concerning electronic information carriers is made. The formation of this case in the investigative

practice is extremely doubtful, since a decision on the appointment of a forensic examination in relation to electronic media can be made only after its inspection and seizure.

It is extremely important to emphasize that based on the position expressed by the legislator in paragraph 1 of part 1 of article 164.1 of the Code of criminal procedure, the formal basis for the seizure of an electronic data carrier is an already prepared decision on the appointment of a forensic examination (accordingly, the protocol of familiarization with the decision should also be provided for familiarization to interested persons).

Paradoxically, in this case, the formal basis for making a decision on the appointment of a forensic examination is the protocol of the investigative inspection, search, seizure, during which the objects of research – electronic data carriers-were discovered, recorded and seized. We dare to assume that such a situation will be formed extremely rarely and in the investigation of criminal cases in the conditions of the created public response.

With the second exception, the legislator designates a situation where the seizure of electronic media is made on the basis of a court decision. But so far, there is a controversial practice on this issue of judicial authorization of the inspection of the contents of mobile phones. One example of the problematic nature of this issue is the precedent created in practice in the Primorsky Territory in 2016.

The investigator appealed to the court with a request for permission to examine the information contained on electronic data carriers, which the Frunzensky District Court of the city of Vladivostok was left without satisfaction. The Court of Appeal upheld the decision. According to the judge, the examination of the information on the electronic media seized from V. is carried out by the investigator in accordance with Article 176 of the Criminal Procedure Code of the Russian Federation and, for this, a court decision is not required (The Primorsky regional court of Russian Federation, 2016).

Later the Constitutional Court of the Russian Federation explained that, if during the inspection of the mobile phone owner self-reports installed on his password, expresses readiness to provide a printout of telephone connections from the number used by him, does not object to the study of the messages available in the phone and information about telephone connections, a violation of constitutional law is not seen (The Constitutional Court of the Russian Federation, 2017).

Meanwhile, according to the position expressed by the Constitutional Court of the Russian Federation in the ruling of 25.01.2018 № 189-O, conducting an inspection and examination in order to obtain information relevant to the criminal case that is in the electronic memory of subscriber devices seized during

investigative actions in accordance with the procedure established by law does not imply making a special court decision. (The Constitutional Court of the Russian Federation, 2018).

So, there are reasons to assume that electronic media may be seized in accordance with paragraph 2 of part 1 of article 164.1 of the Criminal Procedure Code of the Russian Federation in case of receiving the court decision for the investigation, the scope of which is outlined in the norms of article 29 of the Code of Criminal Procedure.

It should be noted that, the American practice is quite consistent in this matter. Thus, on June 25, 2014, the US Supreme Court in its decision in the case of Riley v. California (Riley v. California) ruled that mobile communication devices should be seized only by a court decision.

At the same time, the court's decision was significantly influenced by the opinion of Stanford University law Professor Jeffrey L. Fisher, who acted on behalf of the applicant, David Riley.

J. Fisher notes that

> "very, very profound problems with searching a smartphone without a warrant» and that it was like giving «police officers authority to search through the private papers and the drawers and bureaus and cabinets of somebody's house. The Professor also warned the judges: «every American's entire life to the police department, not just at the scene but later at the station house and downloaded into their computer forever" (The US Supreme Court, 2014).

Meanwhile, the judicial practice of Belgium was formed in a different way. The victim's representative alleged a violation of article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms by the investigator in the course of examining the contents of the applicant's mobile device without a court order.

However, the court of first instance recognized the actions of the investigator as lawful, on the basis that, according to Article 88 ter §1 of the Belgian Code of Criminal Procedure, the investigator can inspect the information system without the court's approval if there is a threat of loss of evidence, or the investigator has good reasons to assume that the information system contains the necessary evidence. On 10 October 2014, the Belgian Court of Appeal issued a decision on the application to declare the investigator's actions illegal.

In particular, it was declared a violation in the course of proceedings is article 8 of the Convention for the protection of human rights and fundamental freedoms, articles 15 and 22 of the Constitution of Belgium, article 28bis §3 of the Belgian code of criminal procedure, article 39bis §3 CCP Belgium, article

88ter of §1 of the criminal procedure code of Belgium, article 88ter §3 of the criminal procedure code of Belgium. Violations consisted of non-compliance with the following established procedures:

- The seizure is carried out strictly in accordance with the procedure established by law and must not violate human rights. Control over the legality of the seizure is carried out by the prosecutor;
- If the necessary information can be withdrawn without removing the information carrier itself, the investigator copies the data to another information storage device;
- If the investigating judge has issued a permit to inspect a certain information system, the necessary procedural actions may also be performed in relation to other devices located in a different location, but connected with this system;
- If the necessary information is stored in the territory of another state, this information is subject only to copying (Muratova, Sergeev, 2020).

The investigating judge, through the prosecutor's office, informs the Ministry of Justice about this, which in turn informs about the necessary investigative actions carried out by the representative body of this foreign state. The victim's representative alleged a violation of article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms by the investigator in the course of examining the contents of the applicant's mobile device without a court order.

However, on February 11, 2015, the court of Cassation recognized the investigator's actions as lawful, since according to Article 88ter §1 of the Belgian Code of Criminal Procedure, the investigator can inspect the information system without court approval if there is a threat of loss of evidence, or the investigator has good reasons to assume that the information system contains the necessary evidence (The Court of Cassation of Belgium, 2015).

The Russian Code of Criminal Procedure provides for three exceptions. The first case of exclusion is possible when electronic data carriers contain information that the owner of the electronic data carrier does not have the authority to store and use. In this case, it is assumed that the electronic data carriers that (or the information on which) are held by the owner due to the illegal actions committed by them will be seized. For example, if counterfeit licensed software is recorded on electronic media with the help of special equipment.

The following exception indicates the case when the information contained on electronic media can be used to commit new crimes. Evidence of such use can be operational-significant and evidential information.

Also, an exception may be a situation in which copying information at the request of a specialist may lead to its loss or change. When carrying out the seizure of electronic media, the conclusion about the possible loss or change of information is made only by a specialist involved in the investigative action. At the same time, this conclusion is expressed in a statement, which is recorded in the protocol of the investigative action during which the seizure was carried out. The absence of an appropriate record that the copying cannot be carried out due to the possible loss or change of information is the basis for recognizing the actions of persons who seize electronic media as inadmissible (Bulgakova, Bulgakov et el., 2019).

On March 13, 2018, the Kamchatka Regional Court found illegal the actions of the detective, expressed in the refusal to satisfy the request of the general director of the enterprise to copy the information seized from electronic media during the search. As it followed from the materials presented to the court, the search report recorded S.'s explanation that the seizure of electronic data carriers (hard drives) completely paralyzes the operation of the enterprise. During the court session he confirmed that he asked the police officers to copy the information seized on electronic media, offered to do this with his own electronic media free of information, but was refused. He wanted to write comments about this in the protocol, but he was not allowed to do so.

Taking into account that the search report does not contain any information indicating that copying the information seized from electronic media may hinder the investigation or lead to its loss or change, the court of appeal concluded that the actions of the official who conducted the search did not fully comply with the provisions of the criminal procedure legislation (the Kamchatka regional court, 2018).

THE NEED TO ATTRACT A SPECIALIST

Part 2 of Article 164.1 of the Code of Criminal Procedure contains the provisions of the law on the mandatory participation of a specialist in the seizure of electronic media. Electronic data carriers are seized in the course of investigative actions with the participation of a specialist. At the request of the legal owner of the seized electronic media or the owner of the information contained therein, a specialist copies the information from the seized electronic media. Information is copied to other electronic media provided by the legal owner of the seized electronic media or the owner of the information contained therein. The special entry about ones is made in Protocol of investigative action.

At the same time, the legislator leaves out of sight the urgent questions – which media belong to this category and whether it is necessary to differentiate

the procedure for removing information from copying during investigative actions.

As has been repeatedly mentioned (Knyazkov, 2018), (Ivanov, 2018), (Vasyukov, Gavrilov, Kuznetsov, 2017), the lack of clarity of these issues has led to numerous scientific discussions (Gavrilin, 2017), (Gavrilov, 2018) and ambiguous court decisions.

In one case, the courts conclude that the participation of a specialist is mandatory only when copying the information contained on the seized items (The Samara regional court, 2018). In another, it is explained that " the participation of a specialist in the production of a seizure during the seizure of electronic media is required if there is a need for this specialist. In fact, during the seizure, the electronic media was not seized, but the available information was copied to a separate medium, which is not prohibited by the norms of the Criminal Procedure Code of the Russian Federation and does not require the mandatory involvement of a specialist" (The Ryazan regional court, 2018).

In the third case, the court recognizes the absence of a specialist as permissible during investigative actions, since "electronic media were seized entirely, that is, without checking and withdrawing the information itself", which does not give the court grounds to doubt the reliability of the information that can later be found in this medium (The Yaroslavl regional court, 2017).

In the fourth case, the court considered unfounded and not to be satisfied the arguments of the appeal about the violation during the search provisions on the mandatory participation of a specialist, because, in the opinion of the judges, "the application of special knowledge and skills in the seizure of a computer block, a part of which is an electronic storage medium, without its opening or copying is not required" (The Supreme Court of Republic Khakassia, 2018).

CONCLUSIONS

Due to the different interpretation by the courts of the need to use special knowledge in the seizure of electronic media, further enforcement of the rules of "electronic seizure" will be accompanied by even greater difficulties. This is due to the fact that the law provides for the mandatory participation of a specialist in the production of an investigative action in the event of the seizure of all types and types of electronic devices where information can be accumulated and stored.

Given the prevalence of electronic media, this rule will lead to the fact that specialists will be more involved in the production of investigative actions than to conduct computer examinations. Therefore, it is necessary to increase the number of experts of state institutions, taking into account their possible relevance in the detection and investigation of crimes.

REFERENCES

THE CONSTITUTIONAL COURT OF THE RUSSIAN FEDERATION. *On refusal to accept for consideration the complaint of the citizen Popov Anatoly Nikolaevich on violation of his constitutional rights articles 176 and 177 of the Criminal procedure code of the Russian Federation:* definition of 28.02.2017 no. 338-O. Available at: http://www.consultant.ru/search/?q=egr+ha.

_____. *On refusal to accept for consideration the complaint of the citizen Prozorovsky Dmitry Alexandrovich on violation of his constitutional rights articles 176, 177 and 195 of the code of Criminal procedure of the Russian Federation*: definition of the constitutional Court of the Russian Federation of 25.01.2018 no. 189-O. Available at: http://www.consultant.ru/search/?q=egr+ha.

THE PRIMORSKY REGIONAL COURT. *Appeal decision in case no. 22-3453/2016*. Available at: http://www.consultant.ru/search/?q=egr+ha.

THE SAMARA REGIONAL COURT. Appeal decision in case no. 22-7165/2018 of 10.12.2018. Available at: http://www.consultant.ru/search/?q=egr+ha.

THE RYAZAN REGIONAL COURT. *Appeal decision in case no. 22-148/2018 of 03.04.2018.* Available at: http://www.consultant.ru/search/?q=egr+ha.

THE YAROSLAVL REGIONAL COURT. *Appeal decision in case no. 22-968/2017 of 11.07.2017.* Available at: http://www.consultant.ru/search/?q=egr+ha.

THE SUPREME COURT OF REPUBLIC KHAKASSIA. *Appeal decision in case no. 22-1516/2018 of 13.12.2018.* Available at: http://www.consultant.ru/search/?q=egr+ha.

THE KAMCHATKA REGIONAL COURT. *Appeal decision in case no. 22k-160/2018 of 13.03.2018.* Available at: http://www.consultant.ru/search/?q=egr+ha.

INVESTIGATIVE COMMITTEE OF THE RUSSIAN FEDERATION. *Extended operational meeting on the development of the Criminal center of the Russian IC* on October 28, 2018. Available at: https://sledcom.ru/news/item/1266876.

KNYAZKOV, A. S. Complicity in the illegal sale of drugs and their analogues, committed through the use of electronic and information and telecommunication networks. *Bulletin of Tomsk State University. Law*, no. 30, p. 53-66, 2018. DOI: 10.17223/22253513/30/5

IVANOV, A. Situational aspects of the study of the identity of the suspect (accused) during the investigation with his participation. *Bulletin of Tomsk State University. Law*, no. 27, p. 30-37, 2018. DOI: 10.17223/22253513/27/3

VASYUKOV, V. F.; GAVRILOV, B. YA.; KUZNETSOV, A. A. *Methods of obtaining evidence and information in connection with the detection (possibility of detection) of electronic media.* Moscow: Prospect, 2017.

GAVRILIN, YU.V. Electronic media in criminal prosecution. *Proceedings of the Academy of Management of the Ministry of Internal Affairs of Russia*, v. 4, n. 44, p. 45-50, 2017.

GAVRILOV, B.YA. Obtaining evidence and information from electronic media: issues of legislative regulation and law enforcement. *Criminal proceedings: problems of theory and practice*. v. 3, no. 3, p. 32-36, 2018.

KOLYCHEVA, A.N. *Fixation of evidentiary information stored on the resources of the Internet.* Moscow, 2019.

U. S. SUPREME COURT. *Riley V. California, 573 U. S.* (2014) Available at: https://supreme.justia.com/cases/federal/us/573/13-132/.

CRIMINAL PROCEDURE CODE OF BELGIUM on 19 November 1808. *Meeting of the legislation of Belgium.* Belgium VRGCodex, 2017-2018.

THE COURT OF CASSATION OF BELGIUM. *The Decision No. p. 14.1739.F/1 of 11.02.2015.* Archive of the court of cassation of Belgium, Antwerpen.

MURATOVA, N.G.; SERGEEV, M.S. *Legal regulation of the use of electronic information and electronic media in criminal proceeding*: domestic and foreign experience. Moscow, Yurlitinform, 2019.

BULGAKOVA, E.; BULGAKOV, V.; TRUSHCHENKOV, I.; VASILIEV, D.; KRAVETS, E. Big data in the investigation and prevention of crimes. *In The world of Big Data: problems of legislation and management technology. Research in systems, decision-making and management*, v.181. Springer, Cham, p. 61-69, 2019. DOI: 10.1007/978.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET