International Journal of Innovation, Creativity and Change. www.ijicc.net
Volume 7, Issue 12, 2019

Legal Regulation of Seizure of Electronic Media in Investigative Action

Lyudmila A. Spektor[a*], Pavel O. Mititanidi[b], Evgeniy V. Zatulivetrov[c], Kirill S. Tsibart[d], Rodion D. Zhmurko[e], Konstantin A. Aleksandrov[f],
[a,b,c,d,e,f]Institute of the Service Sector and Entrepreneurship, DGTU in Shakhty, Russia Shakhty, 147, Shevchenko, 346500, Email: [a*]spektor2@yandex.ru

This article discusses the legal nature and significance of seizure as a procedural action aimed at state-power withdrawal of electronic media, objects or documents relevant to a criminal case.

Key words: *Electronic media, criminal procedure, enforcement agencies, investigative actions.*

Introduction

In modern conditions, the entrepreneurial activity of almost any enterprise is difficult to imagine without the use of information technology. The application of information or digital technology includes, huge volumes of commercial information necessary for normal operation being stored on servers and hard drives on a personal computer; accounting is performed using the 1C program, interaction with the bank occurs via the Internet and personal access keys to the so-called Bank-Client system. Moreover, quite often entrepreneurial activity itself is based on the use of information technology achievements, for example, online stores selling goods, reservation services, etc.

In the case of a forced unexpected seizure of documents, including electronic media, during investigative and operational actions of law enforcement agencies, the activities of organisations are almost paralysed. The President of the Russian Federation V.V. has repeatedly paid attention to this problem. Putin, for example, in August 2017 at a meeting on investment programs for the development of the Far East, he pointed out the need in principle to prohibit law enforcement agencies from seizing servers and hard drives during investigative activities of enterprises. “If it is necessary for the investigation,” the head of state noted, “it is enough to make copies, assure them and use them during the investigation.”

Numerous complaints from representatives of the business community have caused repeated attempts to legislatively regulate this sphere of relations in order to minimise the adverse effects for entrepreneurs. So, by the Federal Law of July 28, 2012 No. 143-ФЗ in Art. 183 of the Code of Criminal Procedure of the Russian Federation, part 3.1 was introduced, establishing a special procedure for the removal of electronic information carriers. This norm provided, in particular, that the removal of the specified medium should be carried out exclusively in the presence of a specialist, at the request of the legal owner of the medium, he should be given the opportunity to copy the information contained on it.

A similar norm in the form of h. 9.1 was included in Art. 182 Code of Criminal Procedure, which regulates the search.

Moreover, in paragraph 20 on the Instructions of the procedure for conducting by the internal affairs bodies of the Russian Federation a public operational-search measure, inspection of premises, buildings, structures, terrains and vehicles, approved by Order of the Ministry of Internal Affairs of the Russian Federation No. 199 of April 1, 2014, establishes such as a matter of fact, as set forth, the rules for the seizure of electronic information carriers during operational-search measures. These standards had some positive effect, however, in my opinion, did not solve the problem.

Despite the fact that law enforcement officers formally proposed to representatives of the organisations in which the investigative actions were performed that they could copy the information available on an electronic medium, there was practically no real possibility for this. It is rare that a company had a spare storage medium of the required volume, a specialist who could copy the information, and also the time necessary for this (often at least 4-5 hours). Thus, in my opinion, these norms, having proclaimed principles that are essentially correct, did not lead to a real result.

Subsequently, the Federal Law of December 27, 2018 No. 533-FZ (hereinafter referred to as the Law No. 533-FZ) of the norm of Part 9.1 of Art. 182, part 3.1 of art. 183 Code of Criminal Procedure were declared null and void. To replace these norms with more effective ones, the same Law No. 533-ФЗ introduced the Art. 164.1 "Features of the removal of electronic information carriers and copying information from them in the course of investigative actions."

The specified norm, in fact, largely repeats the provisions of the expired part 9.1 of Art. 182, part 3.1 of art. 183 of the Code of Criminal Procedure of the Russian Federation with regard to the mandatory participation of a specialist in the removal of an electronic information carrier, providing the holder with the opportunity to use this specialist to copy information to the carrier provided by him, etc. In addition, for the first time, the legislator provided for the

right of the investigator to copy information from electronic media without removing the media itself. However, as practice shows for a short period of validity of this rule, the investigators practically do not use the named right.

However, it should be noted that Art. 164.1 of the Code of Criminal Procedure of the Russian Federation contains a ban on the seizure of electronic storage media, however, this prohibition applies exclusively to cases of seizure during criminal proceedings on crimes under Part 1-4 of Art. 159, 159.1–159.3, 159.5, 159.6, 160, 165 of the Criminal Code of the Russian Federation, if these crimes are committed in the field of entrepreneurial activity, as well as h. 5–7 of art. 159, 171, 171.1, 171.3–172.2, 173.1–174.1, 176–178, 180, 181, 183, 185–185.4 and 190–199.4 of the Criminal Code of the Russian Federation.

Moreover, the prohibition does not apply in cases where: a decision has been made to order a forensic examination in relation to electronic information carriers; seizure of electronic storage media is based on a court decision; electronic information carriers contain information whose storage and use rights the owner of the electronic information carrier does not have, or it can be used to commit new crimes, or copying it, according to a specialist, may lead to its loss or change.

Thus, I believe that, despite the legislator moving in the right direction, limiting the effect of Art. 164.1 of the Code of Criminal Procedure of the Russian Federation only within the framework of a criminal case for a small number of crimes, as well as the right of wide discretion to assess certain circumstances, continues to give law enforcement authorities the opportunity to circumvent established bans and seize electronic media without giving their owners a real opportunity to copy information from them.

Moreover, in my opinion, during the development of the legislative framework on this issue, a very important point was missed; as a result, a gap allows law enforcement agencies to seize electronic media without any prohibitions and conditions, even in the absence of a criminal case. So, in accordance with the provisions of Art. 176, 177 of the Code of Criminal Procedure of the Russian Federation, the inspection of the scene of an incident can be carried out before the initiation of a criminal case as part of the verification of a crime report in accordance with Art. 144-145 Code of Criminal Procedure. During the inspection, any objects and documents that, in the opinion of a law enforcement officer, may subsequently be of value to a criminal case, without any prohibitions or restrictions, may be seized. According to the seized documents and objects, as follows from Art. 144 of the Code of Criminal Procedure, an audit and even a forensic examination may be ordered. Thus, before the initiation of a criminal case, when the established Art. 164.1 of the Code of Criminal Procedure of the Russian Federation, prohibitions, all necessary actions for law enforcement agencies have already been completed, a criminal case as such with an evidence base has

been formed, and an entrepreneur, as a rule, is unable to perform his activities for a long period.

This situation seems all the more dangerous because for the inspection of the scene of the incident the law enforcement authorities need only a formal reason - a report on the crime (for example, a statement, a confession, a report on the detection of evidence of a crime), which is enough to start an inspection under Art. 144-145 Code of Criminal Procedure. Thus, in my opinion, the issue under consideration requires the further development of a comprehensive legal regulation with the aim of maximally protecting the rights and legitimate interests of entrepreneurs, as well as eliminating situations of actually forced suspension of their activities during investigative measures.

So, in my opinion, it would be natural to establish a ban in principle at any stage of criminal proceedings (including before the initiation of a criminal case), as well as, within the framework of operational-search measures, to seize electronic media from commercial and non-commercial organisations, from individual entrepreneurs, and replacing this procedure with the procedure for copying the information available to them by law enforcement officers to their media with the participation of specialists from both sides. In exceptional cases, when law enforcement agencies have good reason to believe that the information contained on electronic media can be used to commit new crimes, the seizure should be performed only by a court decision - by analogy with the search in a residential building.

In addition, in this situation, law enforcement officials must either provide a real opportunity to copy information from the seized source (with the necessary time to acquire a similar medium and copy information), or offer their own medium, which the company could use without disrupting its work in the absence of the seized one. Moreover, the legislation should also provide for a specific short period (no more than 15 days), during which the seized information carrier must be returned to the owner in good condition with all the information available on it.

According to sub. 3.1.9 GOST 2.051-2013, the term “electronic medium” means a material medium used to record, store and reproduce information processed using computer technology. In practice, it can be various media: computers, mobile phones, blocks, devices that make up the material part of a computer system, servers, cash registers and other gadgets.

The removal of electronic storage media can be carried out in organisations and homes of citizens for the purpose of investigating various crimes: theft, murder, terrorist acts, abuse of authority, crimes in the field of economic activity (for example, tax evasion by an organisation, money laundering), cyber-crimes, and also during an investigation into the

dissemination of information prohibited in the territory of the Russian Federation (for example, calls for violation of territorial integrity, calls for extremism, and even slander).

For example, in the summer of 2016, the FSB, during a search of the editorial office of Ekho Moskvy radio station, seized correspondence between Ekho's employees and well-known political scientist, journalist Andrei Piontkovsky on the fact that Piontkovsky's article on Chechnya was published on the Ekho's website, which, according to the FSB, contained calls to the violation of the territorial integrity of Russia and provoked an escalation of hatred based on nationality. Piontkovsky left Russia, fearing criminal prosecution. The trend of recognising articles published on the web as "extremist" is growing, which threatens freedom of speech and infringes on the rights of independent media.

In March 2018, in Magadan, police seized telephones and SIM cards from local residents who are in group chats (including the WhatsApp messenger) and social network communities dedicated to the movement supporting the return of the direct mayoral election procedure. Law enforcement authorities seized a phone from a resident of the city of Natalia as part of a criminal investigation under article 319 of the Criminal Code of the Russian Federation on insulting a representative of the authorities, i.e. Head of the city Yuri Grishan. If the "Magadan affair" is further developed, this can adversely affect the freedom of citizens to express their opinion even in group chats, which are available for reading only for their participants. The bodies authorised to seize information carriers for investigation of crimes are the FSB and the Ministry of Internal Affairs.

What you need to know if in your organisation electronic media are seized during a search / seizure:

Grounds for an exemption.

A search and seizure in an organisation are performed on the basis of a resolution of the investigator, which the investigator must present before the search/seizure begins. The seizure and search, in general, are similar: they have common goals (the seizure of objects, tools, equipment, documents, tools relevant to the criminal case), and the procedure is almost the same. The difference between the seizure and the search is that during the seizure, the investigating authority already knows the location of the item to be seized, so a search for this investigative action is not intended.

The seizure of objects and documents containing state or other secrets protected by federal laws, objects and documents containing information on deposits and accounts of citizens with banks and other credit organisations, as well as things pledged or deposited in a pawnshop, is based on a court decision.

Seizure procedure.
Search and seizure must be performed in the presence of witnesses and a record must be kept. Law enforcement authorities do not warn about the search/seizure in advance, surprise is their key tactical device, because the purpose of the investigative action is to timely find and seize electronic media that are important for the case.

The owner of an electronic medium or the owner of information located on an electronic medium has the right to obtain a copy of the information located on seized media by copying it to other electronic information carriers. This is recorded in the protocol. When making a seizure, it is not allowed to copy information if this can impede the investigation of a crime or, according to a specialist, entail the loss or change of information. According to the meaning of the law, this means that the investigator must justify the refusal to copy information. You also have the right to receive copies at the request after the search/seizure is carried out in the manner prescribed by Art. 81.1 of the Code of Criminal Procedure and Government Decision No. 481 of April 22, 2017

The law does not oblige the owner of electronic media to provide passwords for access to information on media or keys for decryption. The articles of the Code of Criminal Procedure of the Russian Federation on search and seizure (182, 183 of the Code of Criminal Procedure of the Russian Federation) mention a specialist who is involved in the seizure of information carriers. His presence is not necessary, it is the investigator's right to attract a specialist, but not an obligation (Article 168 of the Code of Criminal Procedure of the Russian Federation). As a rule, the investigator needs sufficient general forensic knowledge to detect, fix, and remove a computer unit, laptop, or memory card.

Return of electronic media.
Electronic storage media may be returned if they are not recognised as physical evidence (Article 81.1 of the Code of Criminal Procedure of the Russian Federation). The term for recognition of carriers as material evidence is from 10 to 30 days (Clause 2, Article 81.1 of the Code of Criminal Procedure of the Russian Federation). In the case of the appointment of a forensic examination on the recognition or non-recognition of carriers as material evidence, the period for their return shall accordingly increase by the period of the examination.

If your electronic media is not recognised as material evidence, it must be returned no later than 5 days from the date of the return order.

The news of the Ministry of Justice seems to be good news for organisations to prohibit law enforcement agencies from blocking the work of firms during the preliminary investigation, seizing their equipment and electronic media. Indeed, the seizure and seizure of electronic media often deprives the entrepreneur of the opportunity to continue working during

investigative actions. The agency began developing a bill on behalf of the president. The President, commenting on the seizure of computers at enterprises during the investigative actions, noted: “We need some kind of evidence base - make copies”, it is unacceptable to open the accounts of the enterprise or create other problems in its work. Search/seizure of electronic media in a citizen’s home is according to a similar procedure, but only a court decision made in accordance with Art. 165 Code of Criminal Procedure.

Forensic computer-technical examination.

If necessary, the investigator may order a forensic computer-technical examination (CTE) in relation to the electronic storage media seized during the investigative actions, as a result of which a decision is made (Article 195 of the Code of Criminal Procedure). The examination is carried out by state forensic experts and other experts from among persons with special knowledge. Most examinations are carried out in state forensic institutions organised in the system of federal executive bodies - the Ministry of Justice of Russia and the Ministry of Health of the Russian Federation.

The goals of the CTE: to identify and study the role of the seized information carrier in the crime under investigation; search, detection, analysis and evaluation of forensic information on electronic media.

Types of CTE: hardware-computer (examination of technical (hardware) means of a computer system), computer-software (examination of source code, software), information-computer (examination of data: text, graphics, audio, video, documents, etc.).

Questions for the CTE are posed by the investigator appointing the forensic examination. Depending on the type of crime being investigated, the following can be set:

– What type of information (explicit, hidden, deleted, archived);
– Type of information identified (text, graphic, database, tables);
– How is access (free, limited) to data on the storage medium organized, what are its characteristics;
– Questions about the circumstances of the user's work (chronology of site visits, functioning of email, correspondence and exchange of information in Internet messengers);
– Questions about copyright infringement;
– Questions about the availability of illegal information (for example, child pornography);
– Questions about the presence of malicious software or unlicensed software;
– In general, questions are posed regarding the availability of information relevant to the crime being investigated.

For example, in the case of the arrest of mathematician Dmitry Bogatov (a prisoner of Thor), who was detained on suspicion of distributing calls for participation in an uncoordinated protest and calls for terrorism, Bogatov's computer equipment was seized and complex computer-technical forensics were ordered. Accordingly, questions were raised about the presence of unlawful materials and evidence in the seized equipment linking Bogatov with calls for terrorism and an uncoordinated action published on the forum of the sysadmins.ru site by the user "Airat Bashirov". The examinations lasted 8 months; as a result, no illegal materials and evidence were found that linked Bogatov with the alleged crimes.

We indicated above that gaining access to correspondence and its analysis can also be included in CTE, which potentially violates the right to confidentiality of correspondence, telephone conversations, mail, telegraph and other messages guaranteed by Article 23 of the Constitution of the Russian Federation. In January 2018, the Constitutional Court of the Russian Federation in its determination indicated that conducting an inspection (Article 177 of the Code of Criminal Procedure of the Russian Federation) and examination of the information stored in the electronic memory of seized subscriber devices does not imply a special court decision. Thus, the investigator can gain access to correspondence on the basis of a decision made by him. The decision of the Constitutional Court was made following a complaint by Dmitry Prozorovsky, who is serving a sentence of imprisonment. The applicant contested three articles of the Code of Criminal Procedure of the Russian Federation - "Grounds for the inspection" (Article 176 of the Code of Criminal Procedure), "Procedure for the inspection" (Article 177 of the Code of Criminal Procedure) and "Procedure for the appointment of a forensic examination" (Article 195 of the Code of Criminal Procedure). The complaint stated that the provisions of these articles did not immediately correspond to the six articles of the Constitution of the Russian Federation, since, according to him, they violate the right to confidentiality of correspondence, mail, telegraph and other messages. Such a position of the Constitutional Court creates risks of information leakage to third parties or unfair competitors, as a result of which irreparable harm will be caused to the honor, dignity and reputation of a citizen or business. There is an opposite opinion that this definition of the Constitutional Court of the Russian Federation helps to simplify the procedure for the seizure of electronic media and communications, and also minimises the risk of destruction of evidence of the charge. In any case, it is recommended to set passwords on any digital storage media and encrypt the contents.

The development of digital technology has led to the prosperity of cybercrime and the emergence of new forms of illegal behavior on the network, the means of which are electronic media. The number of seizures and searches is growing, the search and seizure of digital evidence is becoming increasingly important in crime investigations, but the seizure of electronic media is not always justified. Therefore, it is important to know your rights and procedure during sudden visits by law enforcement officers, and you also need to take care of

the internal data protection in advance, for example, keep a backup copy of the data, use cloud data storages so as not to lose the significant information you need for work and other needs.

REFERENCES

Aktual'nye problemy ugolovnogo prava [Actual problems of criminal law]. Textbook / A.V. Groshev et al.: Prospect, 2016 .-- 560 p.

Borovikov, V. B. Ugolovnoe pravo. Obshchaya chast' [Criminal law. A common part]. Textbook / V.B. Borovikov, A.A. Smerdov. - M .: Yurayt, 2015 .-- 212 p.

Brilliantov, A. V. Ugolovno-ispolnitel'noe pravo Rossijskoj Federacii [Criminal-executive law of the Russian Federation] / A.V. Brilliantov, S.I. Kurganov. - M.: Prospect, 2013 .-374 p.

Brilliantov, A. V. Ugolovnoe pravo Rossii v skhemah i opredeleniyah [Criminal law of Russia in schemes and definitions]. Textbook / A.V. Brilliantov, J.E. Ivanova. - M.: Prospect, 2014 .-- 240 p.

Duyunov, V.K. Kvalifikaciya prestuplenij. Zakonodatel'stvo, teoriya, sudebnaya praktika [Qualification of crimes. Legislation, theory, judicial practice] / V.K. Duyunov, A.G. Khlebushkin. - M .: Infra-M, RIOR, 2013 .-- 372 c