https://doi.org/10.25143/socr.15.2019.3.008-023

Use of Information from Electronic Media in Criminal Proceeding of Several European States: Comparative Legal Research

***Andrii Skrypnyk**, Ph.D. researcher*

Yaroslav Mudryi National Law University, Ukraine, Kharkiv
antey.pl@gmail.com

***Ivan Titko**, Prof., Ph.D. (Doctor of Juridical Sciences)*

Poltava Law Institute of Yaroslav Mudryi National Law University, Ukraine, Poltava
titko.iv@gmail.com

Abstract

Investigation of criminal offenses is becoming increasingly associated with the use of information in electronic form. Electronic evidence becomes an integral part of the normative basis of criminal proceeding. The article is devoted to the comparative legal study of the use of information from electronic media in criminal proceeding of several European states. First, the experience of "classical" states of the continental legal system (France, Germany, and Italy) was highlighted. Further, the study of the Baltic region states experience was carried out in relation to each of the states not in isolation, but according to the most favorable structure for comparison. After that some general trends and the most striking problems with the subject were shown. General conclusions related both to signs of electronic evidence and to the most demanded procedural mechanisms for obtaining such data were made.

Keywords: comparative criminal process, electronic evidence, electronic information, investigative actions.

Introduction

Development of information technology greatly affects all spheres of public life. Criminal justice is not an exception. Regulated sources of evidence and procedural tools

for their reception can no longer ignore the enormous amount of electronic data containing unique information for crime disclosure. At the same time, each legal system adapts to modern conditions in different ways.

In view of the similarity of the legal systems elements within the Romano-Germanic (continental) legal family, the comparative legal study of the states belonging to it is especially valuable. The choice of individual states is due to the following reasons: 1) the legal systems of France, Federal Republic of Germany and Italy traditionally belong to the same group or legal family [7, *116–117*]; 2) the legal systems of the Baltic region countries (Estonia, Latvia and Lithuania), having undergone the long-term influence of the socialist system, nevertheless, have made significant progress in the implementation of human rights standards, in particular in criminal proceeding.[1]

Given the objective complexity of forming a systemic view of electronic evidence in the criminal proceeding of foreign countries solely on the basis of the primary material (including considering the language barrier), the primary sources of information (regulations and practice), and modern works of scientists of the respective states have become the benchmarks in the comparative study.

The algorithm of foreign experience study is compiled according to the most expedient, in our opinion, sequence: 1) legal regulation; 2) the place of electronic evidence in the system of evidence sources; 3) problematic issues of observance of human rights and freedoms; 4) public and secret investigative actions that can provide electronic evidence obtaining. In the study of foreign experience, the priority is given to legal regulations with the addition of useful provisions of judicial practice.

Based on the study of foreign experience, we have formed conclusions with the simultaneous identification of general trends and the most pressing problems of electronic evidence use in the field of criminal justice in order to lay the groundwork for further scientific research in the given direction.

Experience of "classical" states of the continental legal family

France

The Criminal Procedure Legislation of the French Republic does not contain the concept of *electronic evidence* or *digital evidence*. Instead, the French criminal justice authorities identify several aspects related to digital data and their use in law enforcement.

Each aspect follows from the relevant regulatory framework: (1) Postal and Electronic Communications Code (*Code des Postes et des communications électroniques*) identifies obligations relevant to Internet service providers *vis-à-vis* individual users and

[1] For example, Estonia's high position in the ranking of states under the rule of law index can serve as confirmation. (https://gtmarket.ru/research/rule-of-law-index/info).

public authorities; (2) Criminal Code (*Code pénal*) defines crimes and offences committed against or through the use of information and communication systems; (3) Criminal Procedure Code (*Code de procedure pénale*) frames the legal requirements for digital evidence collection; (4) Internal Security Code (*Code de la sécurité intérieure*) defines how intelligence agencies can collect information and data for the purpose of maintaining security and countering terrorism [11, *15–16*].

The French Code of Criminal Procedure (hereinafter referred to as the FCCP) provides the possibility to use criminal evidence in information and communication systems (Art. 94 of the FCCP).

At the same time there is a differentiation of procedural order of access to: (electronic communications; digital data, [11, *17*; 2, *277*] in particular:

a) regarding the electronic form of communication, the procedural law determines, *firstly,* the conditions under which law enforcement authorities may initiate the interception of communicative information (Article 100-100-7 of the FCCP), and *secondly*, the list of data that can be obtained (Article 706-95-706-95-10). The specification of the mentioned procedural rules was found in the Postal and Electronic Communications Code, which obliges Internet service providers: (1) to collect and store communication data for one year, the list of which is exhaustive (Art. L34-1, R10-13 of the FCCP); (2) to provide such information to law enforcement authorities only for the purpose of a criminal investigation, and only in the case of a request [11, *17–18*]. The refusal to provide data on request results in fine imposition [2, *276*];
b) in general terms, procedural regulation of digital data obtaining is as follows. *Firstly,* the French investigation authorities are authorised to implement a technical device, capable of recording, storing and transmitting information to the relevant authorities, to the information system of the user without his consent (Art. 706-102-1 of the FCCP) [11, *17*]. The term *dispositif technique* used in this rule covers a large variety of tools, but it is mostly related to Trojans. Such procedural action can only be carried out by permission of the court to investigate crimes that, according to the qualifications of the European Court of Human Rights, may be attributed to serious criminal activity [3]. *Secondly*, in proceedings concerning a separate category of crimes, the possibility of decrypting data protected by information security systems is foreseen, subject to prior permission of the prosecutor or the court (Art.230-1-230-5 of the FCCP) [3]. *Thirdly*, law enforcement agencies are authorised to gain access to geographical localisation of any object deemed relevant to criminal investigations (Art. 230-32-230-44 of the FCCP) [3].

Thus, the French legislation covers the full range of possible cases of obtaining and using digital evidence, with the simultaneous installation of information security guarantees introduced in the *Act on Information Technology, Data and Civil Liberties* in 1978 [21].

Germany

Legal basis of electronic form of evidence-based information use in the Federal Republic of Germany (hereinafter – Germany) makes up the German Code of Criminal Procedure (*Strafprozeßordnung*) (hereinafter – the GCCP) [13], certain provisions of the Federal Criminal Police Office Act) (*Bundeskriminalamtgesetz*) [14], the Telecommunications Act (*Telekommunikationsgesetz*) [25]. Similar to the FCCP, the GCCP, although not using or reinforcing the concept of *electronic evidence* or *digital evidence,* contains provisions that can be applied to information in electronic form, especially in terms of its defense during the investigation [20, *27*]. For example, such standards include: the prohibition on seizure of written communications or any information about them if their holder has the right to refuse to testify (Sec. 1 Par. 97 of the GCCP); the prohibition on seizure of audio recordings, image recordings, information, photographs and other works owned by journalists and the media (Sec. 5 Par. 97 of the GCCP) [13].

Investigating procedural tools, we should touch the coverage of the constitutional aspect, especially in terms of human rights and freedoms observance. Thus, the body of constitutional control of Germany, on the basis of the systematic combination of two constitutional values: human dignity (Art. 1 of the German Basic Law) and self-development (freedom) of an individual (Par. 1 Art. 2 of the German Basic Law), has developed a new concept of the right to privacy in the digital space. In its decision, the court named it as the right to the guarantee of the integrity and confidentiality of information technology systems [11, *36*]. The Federal Constitutional Court of Germany noted that the secret access to the information and technology system, which consists in actions monitoring of the system user or information reading, can be considered valid only in the presence of factual data on the threat to the protected interests of higher, compared with private, priority level [17]. Thus, the constitutional control body of Germany has extended the legal protection of guarantee of the right to privacy of correspondence, postal items and telecommunications (Art. 10 of the German Basic Law), extending its validity and information generated and stored on electronic devices [11, *36*].

In the context of collecting information from electronic media, the public tools are: (1) seizure (Sec. 94-98 of the GCCP); (2) automated comparison and transfer of personal data (Sec. 98-98c of the GCCP); (3) request for receiving telecommunication information stored by telecommunication service providers (Sec. 100g, 100j of the GCCP); (4) inspection of documents and electronic media (Sec. 110 of the GCCP).

The most striking features of these actions are as follows:

a) seizure may concern items that can be relevant to the investigation as evidence, in particular computer files and e-mails [15, *139*]. The GCCP does not link the possibility of the seizure with a certain degree of severity of the investigated offence. At the same time, according to the general rule, such procedural action can be carried out on the basis of a court ruling, and only in urgent cases – the decisions of the prosecutor or the investigator on his behalf (Par. 1 Sec. 98

of the GCCP). The specificity of the seizure is that it can only relate to information that is on electronic media, which was previously obtained or created, and then only stored. In the case of the transmission of this information by communication channels, its collection should be carried out within the control of telecommunications (Sec. 100a of the GCCP), which is already a secret investigative action [15, *57–58*];

b) automated comparison and transmission of personal data are based on obtaining and automated processing of personal data bases carried out in order to establish the circle of persons who have important characteristic features for the further investigation (Par. 1 Sec. 98a of the GCCP). In the context of our research, at least three aspects of such investigative action deserve attention. *Firstly*, the establishment of a requirement regarding the gravity and nature of the criminal offence under investigation (Par. 1 Sec. 98a of the GCCP); *secondly*, the conduct of an action using automated information systems (Sec. 98c of the GCCP); *thirdly,* the obligation to return the electronic media to disposers after the end of the data comparison and to delete the copied information (Par. 3 Sec. 98b of the GCCP);

c) request for receiving telecommunication information stored by telecommunication service providers may relate to information about subscribers of telecommunication services (Sec. 111, 113 of the Telecommunications Law (*Telekommunikationsgesetz*)) [25] – according to Sec. 100j of the GCCP, or telecommunication services provided (Sec. 113b of the Telecommunications Law) [25] – according to Sec. 100g of the GCCP. At the same time, such request may not relate to: the data related to the use of e-mail; the data held by over-the-top massaging providers [11, *34*];

d) inspection of documents and electronic media (Par. 1 Sec. 110 of the GCCP) is possible only concerning the documents found during the search. Although this article does not contain general rules for carrying out the inspection of electronic media, there is a special rule devoted to the remote inspection in Par. 3. According to this rule, if there is a threat of stored data loss, it is allowed to conduct an inspection of an electronic medium that does not have physical access, but is available virtually (for example, via a local network).

The tools for secret investigative actions are more diverse. For example, telecommunications control (Sec. 100a, 100b of the GCCP) may be implemented using specially designed software – Bundestrojaner (*Quellen-Telekommunikationsuberwachung*). The specified Trojan programme is not directly foreseen by the GCCP, but it is "legalised" through the provisions of the Federal Criminal Police Act (Sec. 51) [14] as a preventive measure against terrorist threats. The value of such software is the ability to track and record all kinds of real-time electronic communications (such as Skype, instant messaging, e-mails) even before their encryption [11, *30–31*]. And it greatly increases the event efficiency and the reliability of its results. However, the question of the admissibility of evidence obtained using such a Trojan programme (under the so-called online search) is ambiguous in German law enforcement practice [2, *267*; 11, *31*; 15, *167*].

Italy

The use of information from electronic media in the criminal proceeding in Italy is based on the Italian Code of Criminal Procedure (*Codice di procedura penale*) (hereinafter referred to as the ICCP), and in some aspects of the Personal Data Protection Code (*Codice in materia di protezione dei dati personali*) [10] and the Electronic Communications Code (*Codice delle comunicazioni elettroniche*) [9]. Similar to the regulations of France and Germany, Italian criminal procedure legislation does not distinguish "electronic" or "digital evidence" as an independent procedural source.

The ICCP provides procedural tools for evidence collecting from electronic media including the following procedural actions: inspection (Art. 244); search, including "digital" one (cl. 1-bis Art. 244, cl. 1-bis Art. 352); seizure of electronic data (Art. 254-bis); recording and seizure of information in urgent cases (Art. 354).

Their features are considered further:

a) the ICCP does not provide for a separate type of inspection, the object of which is electronic media. However, in the case of information or telecommunication systems, it is envisaged that technical measures should be taken to ensure that the data are unaltered (for example, by disconnecting from a global or local network) [9];
b) regarding the search, the ICCP distinguishes a special kind, the object of which may be electronic media of information, such as digital data, software or other "electronic" traces (cl. 1-bis Art. 247). Such a search is called a "digital" one in the scientific literature [11, *45*]. It is conducted on a motivated permission, if there are reasons to believe that information necessary for the investigation is contained in the information or telecommunication system. At the same time, the person who conducts a "digital" search is responsible for taking technical measures aimed at ensuring the integrity of stored data [8].
c) the electronic data seizure (Art. 254-bis of the ICCP), which is specifically designed to collect evidence from digital sources, is based on the seizure of data from information, telematic and telecommunication service providers. In this case, a particular attention is paid to maintaining the authenticity of the data received. Thus, the originality of digital data should be provided both by providers during collection and storage and by the investigating authorities when copying on electronic media (Art. 254-bis of the ICCP) [8]. It is noteworthy that the range of providers obliged to provide "mandatory services" does not include over-the-top massaging providers and information society services providers[2]

[2] This refers to the services regulated by Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Srvices, in particular Electronic Commerce, in the Internal Market (Directive on electronic commerce) [See Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Srvices, in particular Electronic Commerce, in the Internal Market ('Directive on electronic commerce'). *Official Journal of the European Union* (L 178) 17 July 2000. Available from: http://data.europa.eu/eli/dir/2000/31/oj [Accessed 29 November 2019].

(for example, Google, Facebook, Skype, etc.) [11, *44*]. That is why, according to the described situation, it is advisable not to conduct a seizure, but to apply a mechanism for collecting digital documents and computer data stored abroad (Art. 234-bis of the ICCP);

d) fixing and seizure of information in urgent cases, as one of the urgent inspection types (Art. 354 of the ICCP), are, first of all, of a preventive nature. Their conduct is allowed in the presence of a real threat of destruction or alteration of evidentiary information (digital data, computer programs, and other information from computer or telecommunication systems). The features of this extraordinary investigative action are that it can be carried out: before the beginning of the investigation; by police officers who are not investigators (cl. 2 Art. 344 of the ICCP). At the same time, the police have three main responsibilities: 1) to take all possible measures to keep the information unchanged and to prevent access to it; 2) in the presence of technical capability, to copy the information to the electronic media; 3) if necessary, to remove the electronic media [8].

The tools for secret investigative actions in Italian procedural law are consistent with the traditional one: an interception of conversations (Art. 266 of the ICCP), an interception of computer or telematic communications (Art. 266-bis of the ICCP), a seizure of correspondence, including electronic (Art. 353 of the ICCP) and so on. Given the limited scope of the article, we will try to focus on highlighting only one, but in our opinion, the most problematic aspect is the use of Trojan programs for electronic evidence obtaining [11, *47*]. Trojan programmes are a type of malware that appears to be harmless and deceives the user in order to stimulate an active conduct that will result in its installation on the target computer system [26, *88*]. The ICCP does not directly regulate the legitimacy of the Trojan programmes use during the criminal investigation. At the same time, the possibility of using malware can follow from a number of provisions of the law [1, *8–13*].

Attempts to resolve regulatory uncertainty have been made by the Italian Supreme Court of Cassation and have been consolidated in a number of decisions on this issue.

The position of the court can be conditionally grouped in the following way:

a) there is no secret observation when using Trojans. This conclusion follows from the fact that the investigation body's actions consist solely in the removal and duplication of information stored on the hard disk. That is, the seizure is not any "flow of communications", but "only an operational relationship between the microprocessor and video of the electronic system" (*Italian Supreme Court of Cassation, Division V, Decision № 24695, of 14 October 2009*) [26, *91*];

b) the above position, supported by another decision of the Italian Supreme Court of Cassation (*Italian Supreme Court of Cassation, Division VI, Bisignani Case – Decision No. 254865, of 27 November 2012*), did not remain without further development. Thus, the court recognised the necessity of obtaining a permit from the prosecutor to conduct such a private action [26, *92*];

c) the Italian Supreme Court of Cassation identified the case where the use of the Trojan programme should be considered "invasive and unlawful" (*Italian Supreme Court of Cassation, Division VI, Musumeci Case – Decision No. 27100, of 26 May 2015*) [11, *47*]. This inadmissible interference occurs when the Trojan program collects not the information that is already stored on the media, but the information that is generated on-line and can be captured by the information system (for example, by activating the microphone or video camera of the device, recording the data input by the user);
d) the given categorical conclusion, at the same time, is not absolute. The court recognised the lawful use of Trojan programmes in the way described above without obtaining prior judicial authorization only in the course of an investigation of terrorism or organized crime (*Italian Supreme Court of Cassation, Joint Sessions, Scurato Case – Decision No. 1 July 2016*) [11, *48*].

Thus, being irregularly normative, the issue of using Trojans in the criminal process in Italy is solved as follows: online search [26, *92*] of the information stored is legal and can be carried out subject to the minimum warranty – receiving a permission from the prosecutor, while online surveillance [26, *92*] with the information obtaining that is being transmitted or only being formed, requires a prior judicial authorisation, the lack of which is justified only in the course of the investigation of "serious criminal activity" [16].

Experience of the Baltic states

The Code of Criminal Procedure of the Republic of Lithuania (*Baudžiamojo proceso kodekso*) [6] (hereinafter – the LitCCP) and the Code of Criminal Procedure of the Republic of Estonia (*Kriminaalmenetluse seadustik*) [4] (hereinafter – the ECCP) contain no special principles or rules for collecting evidence from electronic media.[3] At the same time, the legislation of the Baltic States differently solves the issue of the affiliation of electronic evidence to types of procedural sources. According to the LitCCP, electronic evidence can be qualified as documents (cl. 4 Part 1 Art. 96 of the LitCCP). The ECCP provides a non-exhaustive list of evidence sources, including lists and information from electronic media (videos of secret activities, movies and other data records) (Sec. 63 of the ECCP) [4]. According to the ECCP, it can generally be concluded from case law and legal commentary that evidence in digital form is accepted in courts like any "tangible" evidence [22, *109*].

In contrast to the above mentioned, the Code of Criminal Procedure of Latvia (*Kriminālprocesa likums*) [5] (hereinafter – the LatCCP) establishes electronic evidence

[3] In Estonia, this feature is criticised by scientists [See Osula, A.-M., Zoetekouw, M. (2017). The Notification Requirement in Transborder Remote Search and Seizure: Domestic and International Law Perspectives. *Masaryk U.J.L. & Tech.* 11 (1) 103, p.109. Available from: https://doi.org/10.5817/MUJLT2017-1-6 [Accessed 29 November 2018].

as a separate source (Art. 136 of the LatCCP) (as the other "classical" evidence: testimony, physical evidence, documents, etc.). Meanwhile, the Latvian science has suggested the possibility of using electronic data only with electronic media – physical evidence and/or expert opinion drawn up as a result of their research. According to scientists, if the direct study of physical evidence is not possible, electronic evidence can only be used as indirect, and only if it is confirmed by other means of proof [24, *61*].

Proceeding to the study of secret investigative actions, in particular, the LatCCP assumes the following: 1) granting access to information that is processed, stored or transmitted by the electronic information system (upon request, without the possibility of the media seizure) (Art. 190 of the LatCCP); 2) a provisional action is imposing on the information disposer the obligation to keep it unchanged, ensuring its inaccessibility for third parties for up to 30 days (Art. 191 of the LatCCP); 3) the request for information stored in accordance with Art. 191 (Art. 192 of the LatCCP) [5].

The LitCCP establishes slightly different tools. They consist, among other things, of the following investigative actions: 1) access of the prosecutor to information (Art. 155) is a familiarsation with the information content and its copying carried out on the basis of a prosecutor decision made with the consent of the preliminary proceeding judge[4]; 2) inspection with the use of technical means (Part 2 Art. 205 of the LitCCP), which may be carried out not only at the site of the object's detection, but also in the most suitable place for this (from a technical point of view); 3) photographing, video shooting of the accused and other persons at the decision of the prosecutor for the formation of forensic card files (Art. 156 of the LitCCP) [6].

In the criminal proceedings in Estonia, electronic media are obtained as a result of the seizure (Sec. 142) during the search (Sec. 91 of the ECCP). Electronic data are obtained as a result of the search (Sec. 83, 86 of the ECCP) or examination (Sec. 95-109-1 of the ECCP) of the seized media [19, *115*]. At the same time, the possibility of conducting an electronic search in Estonian legislation, doctrine and practice is resolved ambiguously. Based on the provisions of Sec. 91 of the ECCP, the possibility of electronic media seizure during the search is indisputable. At the same time, according to Anna-Maria Osula and Mark Zoetekouw, the right of the investigating authority to carry out a search of the electronic media, guided only by the requirements of Sec. 91 of the ECCP (general rules of search), is quite controversial. However, according to the scientists, it is possible to explore the inner content of electronic media with a combination of investigation – a search (Sec. 91) and the aforementioned inspection (Sec. 83, 86 of the ECCP). At the same time, the combination itself contains variants: the electronic medium detected during the search is inspected immediately; the electronic medium detected during the search is seized, and its examination is carried out later [22, *109–110*]. However,

[4] It is noteworthy that a fine (Part 2 of Art. 155 of the CCP of Lithuania) would be a consequence of the failure of the administrators to grant access to information, similarly to the CCP of France and unlike the CCP of Latvia (Part 2 of Art.190).

the combination described above is not without disadvantages. As E. Laurits rightly points out, an "electronic media search" in the form of the inspection threatens unrestricted interference with privacy. The reasons for this are: unlimited inspection time; conduction without a special permission of a prosecutor or a judge; as a result, there is a lack of grounds substantiation for inspection; the unlimited amount of information that is being inspected [18, *87–88*].

Considering the tools of secret investigative actions; in the criminal proceedings of Latvia, for the secret obtaining of information in electronic form the following actions may be carried out: 1)control of telecommunication networks (Art. 218 of the LatCCP); 2)control of the information stored (Art. 219 of the LatCCP); 3) control of the information transmitted (Art. 220 of the LatCCP).

Particular attention is drawn to the Latvian version of the stored information control. Such secret action allows1) to carry out not only the secret search of the information system (i.e. the search and seizure of stored information), but also the collection of data from the environment (*"datu vides"*) (similar to the Italian version of online surveillance [5]; 2) to delete the data without the knowledge of their owner (Part 1 of Art. 219 of the LatCCP); 3) to access another information system in Latvia without a special judicial authorisation (Part 2 of this Art.).[5]

In the procedural law of Lithuania, a secret investigative action such as the control of information transmitted by telecommunication networks is peculiar (Art. 144 of the LitCCP). Such a means of secret collection of evidence may be conducted during an investigation not only of "serious criminal activity", but also of minor crimes, the list of which is exhaustive. In addition, the control of communicative information is carried out with the risk of applying to the victim of violence, coercion or other unlawful influence, to other participants in the process or their close relatives [6].

We will try to study the most vivid aspects of the secret investigative actions in the criminal process of Estonia from the point of view of enforcement. To do this, we will consider two problems. The first one is related to the procedural order for access to the remote information system. The ECCP provides for the possibility of obtaining evidence from the territory of other states in the framework of international cooperation, which at present is in the form of mutual legal assistance (Sec. 65). At the same time, law enforcement practice of Estonia recognises as lawful the evidence obtaining from the territory of another state without sending a request for legal assistance in case when there is an access to the existing virtual servers of foreign countries. The law enforcement bodies think as follows, "an action (the copying of data) is performed in the territory of Estonia by an Estonian body conducting proceedings, and the data can be received without physically leaving the territory of Estonia; and Estonia has the jurisdiction to copy the data" [19, *118*].

[5] The last procedural possibility resembles a remote digital survey in accordance with § 110 of the CCP of Germany.

The second problem is connected with the limits of establishment of correspondence legal protection, in particular, in the context of electronic communications. Addressing the latter linked to the resolution of two key issues: (1) whether the modern means of electronic communication are under the correspondence protection; (2) whether the privacy expands to the correspondence received by the addressee [[19, *118*]. According to the position of the Supreme Court of the Republic of Estonia, modern means of communication belong to correspondence in the context of the mentioned constitutional guarantee (i.e. the answer to the first question is positive), whereas the privacy ceases to exist after receiving the message by the addressee (i.e. the answer to the second question is negative).[6]

Discussion

The study of experience of the abovementioned European states provides an opportunity to distinguish the following main trends:

a) the effectiveness of the mechanism for obtaining a large mass of information in electronic form is primarily ensured by a qualitative legal regulation of activities of telecommunication services' providers. Such regulation requires consolidation of classification of information; degrees of its protection; algorithms for collection and storage of information; interaction of providers with law enforcement agencies;
b) procedural requirements concerning the following are guarantees of observance of human rights: severity of the criminal offense under investigation; necessity of obtaining a permit of the prosecutor or court for conducting the relevant investigative action;
c) traditional procedural immunities (witness, defender) remain valid for information in electronic form (France, Federal Republic of Germany). The form of information does not reduce the scope of legal protection of its content; therefore, it is possible to talk about the "electronic (digital) immunity" of categories of individuals traditionally entitled to the right to remain silent.

These trends should be taken into account by the rule-makers of those countries where they have not yet found their formalisation.

The research revealed a number of controversial issues:

a) lack of unity in the European space in the matter of determining the place of electronic evidence in the system of other evidence (in some states they are identified as a separate source of evidence (Latvia); in others, they are related to physical evidence (Federal Republic of Germany, Estonia) or documents (Italy, Lithuania). However, the terminology itself is not decisive. Determinants of

[6] For further information see Decision of the Estonian Supreme Court Criminal Chamber dated 30 June 30 2014, No. 3-1-1-14-14; § 816–817.

effectiveness are the accuracy and consistency of legal provisions (including terminology), devoted to the regulation of certain procedural actions, and their adaptation to the specifics of electronic information;

b) existence of various ways of electronic data protecting: extension of the right to privacy in its traditional sense (France); justification of the special right to guarantee the integrity and confidentiality of information technology systems (Federal Republic of Germany). Both approaches are acceptable, but the disadvantage of the first one is the need for normative clarification or the application of a dynamic method of law interpretation;

c) contrast of approaches to the question of maintaining the status of "correspondence" by electronic messages already received by the addressee: from an affirmative response in the doctrine of the Constitutional Court of the Federal Republic of Germany to the negative one in the practice of the Supreme Court of Estonia. In our opinion, the first of these approaches is more acceptable, since, *firstly*, it is aimed at extending the scope of the legal guarantee, and *secondly*, it is consistent with the logic of the protection of not the "location" (telecommunication network or carrier), but the content of information;

d) uncertainty about the limits of privacy in conducting investigative actions aimed at obtaining electronic evidence. One of the most striking aspects was the question of the adaptability of traditional investigative actions. The mentioned issue arose the most acutely in Estonian legal reality, where it was problematic to apply the general rules of inspection and search in the investigation of an electronic medium (without a generally accepted guarantee, a prior permission, which should set the limits of intervention). Therefore, the development of a special type of inspection or search, adapted for information in electronic form, deserves to be supported. The normative basis for such an action should be to ensure a reasonable balance of human rights (prior authorization to determine the exact limits of intervention) and the effectiveness of the pre-trial investigation (the possibility of urgent conduct with the subsequent application for permission). Another important aspect was the validity of data obtained with the help of virus software (Trojan programmes). The "secret" aspect of the problem is: regulatory uncertainty (Italy) or regulation not in the procedural law (Federal Republic of Germany), which gives rise to well-founded doubts about the admissibility of evidence; the possibility of deleting stored data without the knowledge of their owner[7] (Latvia);

[7] Without excluding the expediency of such a power as a preventive measure (for example, in order to prevent a crime from using stored information), we cannot agree with the presence of a similar interest in the evidence activity. If the information is relevant for the investigation, i.e. it is an evidence, then there is no sense in its removal; if it does not have such significance, then the investigating authority has no legal basis for any actions with it.

e) openness of the question of "electronic extra-territoriality" (Latvia, Estonia), in particular the possibility for the state to receive information from servers located in other states in the presence of virtual access to them without the involvement of international instruments of criminal procedural cooperation. The problem is that the mechanisms introduced by the bilateral agreements, due to their complexity and duration, are ineffective with regard to electronic evidence, and the unified European procedure is currently only being developed [see 23]. At the same time, procedural mechanisms should not violate the "electronic" sovereignty of the state. Because of this, the most promising is the unification of procedures for obtaining electronic evidence that should ensure the balance of the effectiveness and inviolability of the state's sovereignty.

Conclusions

The legal status of information from electronic media in the system of evidence sources in the legislation of France, Federal Republic of Germany, Italy, Latvia, Lithuania and Estonia varies: from the attribution of documents or physical evidence to traditional sources, to identification as an independent one. In view of the unique nature of electronic evidence, their identification as a separate procedural source is not capable of ensuring the effectiveness of the investigation and its compliance with human rights standards. *On the one hand*, electronic evidence is already included in the criminal proceeding system with all the consequences of this (the spread of immunities, legal guarantees, etc.), which requires the adaptation of traditional rules to new conditions. *On the other hand*, electronic evidence has its own specifics, ignoring of which can cancel the results of its collection, that, in its turn, requires "normative novelty". Both components should be taken into account when developing procedural mechanisms for collecting information in electronic form. The tools of public and secret procedural measures for obtaining evidence, fixed in foreign codes, are characterised by variation in the content of actions with uniform procedural guarantees. At the same time, the lack of unified international procedures leads to problems when collecting electronic evidence from the territory of other states. The current state of the development of information technology requires the implementation of unified and rapid measures not only within a separate part of the world, as the boundaries and distances of information are not of particular importance for the movement of information. This also can become a promising area for further research.

Elektronisko mediju informācijas izmantošana daudzu Eiropas valstu kriminālprocedūrā: salīdzinošā juridiskā pētniecība

Kopsavilkums

Reglamentētie pierādījumu avoti un procesuālie rīki to saņemšanai vairs nevar ignorēt milzīgo elektronisko datu daudzumu, kas satur unikālu informāciju noziegumu atklāšanai. Tajā pašā laikā katra tiesību sistēma dažādos veidos pielāgojas mūsdienu apstākļiem. Ņemot vērā tiesību sistēmu elementu līdzību rumāņu-ģermāņu (kontinentālajā) juridiskajā saimē, tai piederošo valstu salīdzinošais juridiskais pētījums ir īpaši vērtīgs. Tāpēc salīdzinošajai juridiskajai analīzei tika izvēlētas sešu Eiropas valstu (Francijas, Vācijas Federatīvās Republikas, Itālijas, Igaunijas, Latvijas un Lietuvas) tiesību sistēmas. Ārvalstu pieredzes pētījums tika veikts noteiktā secībā: tiesiskais regulējums; elektronisko pierādījumu vieta pierādījumu avotu sistēmā; cilvēktiesību un brīvību ievērošanas problemātiskie jautājumi; publiskas un slepenas izmeklēšanas darbības, kas var sniegt elektronisku pierādījumu iegūšanu. Tika secināts, ka no elektroniskajiem plašsaziņas līdzekļiem iegūtās informācijas juridiskais statuss pierādījumu avotu sistēmā iepriekš minēto sešu valstu tiesību aktos ir atšķirīgs. No vienas puses, elektroniskie pierādījumi jau ir iekļauti kriminālprocesa sistēmā (ar visām no tā izrietošajām sekām – imunitātes izplatību, tiesiskajām garantijām utt.), kurai ir jāpielāgo tradicionālie noteikumi jauniem nosacījumiem. No otras puses, elektroniskajiem pierādījumiem ir sava specifika, kuras ignorēšana var atcelt to vākšanas rezultātus, kuriem savukārt ir nepieciešami jauni normatīvi. Tiek uzsvērts, ka, izstrādājot procesuālus mehānismus informācijas vākšanai elektroniskā formā, ir jāņem vērā abi aspekti. Nobeigumā tiek secināts, ka vienotu starptautisku procedūru trūkums rada problēmas, vācot elektroniskus pierādījumus no citu valstu teritorijas.

Atslēgvārdi: salīdzinošais kriminālprocess, elektroniskie pierādījumi, elektroniskā informācija, izmeklēšanas darbības.

References

1. Angelosanto, P. (2014). *Le Intercettazioni Telematiche e le Criticita del Data Retention nel Contrasto alla Criminalita Organizzata. Sicurezza e Giustizia*, 4(4), 8–13. Available from: http://www.sicurezzaegiustizia.com/?p=10750 [Accessed 29 November 2019].
2. Bahrii, M. V., Lutsyk, V. V. (2017). *Procedural Aspects of the Secret Reception of Information: Domestic and Foreign Experience*. Kharkiv: Law, p.376.
3. *Code de Procédure Pénale.* (2018). Version Consolidée au 2 Novembre 2018. Art. 706-73, 706-73-1. Available from: https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071154&dateTexte=29990101 [Accessed 29 November 2019].
4. *Code of Criminal Procedure of The Republic of Estonia (Kriminaalmenetluse seadustik), on 12 February 2003*; RT I 2003, 27, 166. Available from: https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/509012019001/consolide [Accessed 29 November 2019].

5. *Criminal Procedure Law of The Republic of Latvia (Kriminālprocesa likums), on 21.04.2005*; Latvijas Vēstnesis, 74 (3232), 11 May 2005. Available from: https://likumi.lv/ta/id/107820-kriminalprocesa-likums [Accessed 12 January 2020].
6. *Code of Criminal Procedure of The Republic of Lithuania (Baudžiamojo proceso kodeksas), on 14 March 2002*; Žin. 2002, No. 37-1341. Available from: https://www.e-tar.lt/portal/lt/legalAct/TAR.EC588C321777/UNqWwsXDMa [Accessed 29 November 2019].
7. David, R., Jauffret-Spinosi, C. (2002). *Les grands systèmes de droit contemporains*. Dalloz, p.600.
8. Decreto del Presidente della Republica 22 Settembre 1988, n. 447 "Approvazione del Codice di Procedura Penale". (GU n. 250 del 24-10-1988 – Suppl. Ordinario n. 92). Available from: http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.del.presidente.della.repubblica:1988-09-22;447 [Accessed 29 November 2019].
9. Decreto Legislativo 1 Agosto 2003, n. 259 "Codice delle Comunicazioni Elettroniche". (GU n. 214 del 15-9-2003 – Suppl. Ordinario n. 150). Available from: http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-08-01;259 [Accessed 29 November 2019].
10. Decreto Legislativo 30 Giugno 2003, n. 196 «Codice in Materia di Protezione dei Dati Personali» (GU n.174 del 29-7-2003 - Suppl. Ordinario n. 123). Available from: http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30;196 [Accessed 29 November 2019].
11. De Zan, T., Autolitano, S. (2016). *EUnited Against Crime: Improving Criminal Justice in European Union Cyberspace*. Roma: Istituto Affari Internazionali, 93.
12. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in particular Electronic Commerce, in the Internal Market (Directive on electronic commerce). *Official Journal of the European Union*. L 178, 17.7.2000, 1–16. Available from: http://data.europa.eu/eli/dir/2000/31/oj [Accessed 29 November 2019].
13. *German Code of Criminal Procedure, 7 April 1987.* (1987). *Federal Law Gazette*. Part I, p. 1074, 1319, with amendments by the Act of 23 April 2014. *Federal Law Gazette*. Part I, 410. Available from: http://www.gesetze-im-internet.de/englisch_stpo [Accessed 29 November 2019].
14. *Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten, 01 Juni 2017.* (2017). Available from: https://www.bka.de/SharedDocs/Downloads/DE/DasBKA/Auftrag/bkag/bkaGesetz.html [Accessed 25 May 2019].
15. Golovenkov, P., Spitsa, N. (2012). *The German Code of Criminal Procedure – Strafprozessordnung (StPO): Scientific and Practical Commentary and Translation of the Law Text.* Potsdam: Universitätsverlag Potsdam, 408.
16. *Iordachi and Others v. Moldova.* (2009). Application No. 25198/02. European Court of Human Rights, 10 February 2009. Available from: http://hudoc.echr.coe.int/eng?i=001-91245 [Accessed 29 November 2019].
17. Judgment of the First Senate of 27 February 2008, Federal Constitutional Court, 1 BvR 370/07, 1 BvR 595/07. Available from: http://www.bverfg.de/e/rs20080227_1bvr037007en.html [Accessed 29 November 2019].
18. Laurits, E. (2015). Some Problems Encountered in Computer System Searches. *Yearbook of Estonian Courts*, 85–102. Available from: https://www.riigikohus.ee/sites/default/files/elfinder/%C3%B5igusalased%20materjalid/Riigikohtu%20tr%C3%BCkised/Riigikohtu_aastaraamat_eng_veebi.pdf [Accessed 12 January 2020].

19. Laurits, E. (2016). Criminal Procedure and Digital Evidence in Estonia. *Digital Evidence and Electronic Signature Law Review*, 13 (2016). 113–120. Available from: http://dx.doi.org/10.14296/deeslr.v13i0.2301 [Accessed 12 January 2020].
20. Lázaro, C. et. al. (2006). *The Admissability of Electronic Evidence in Court: Fighting Against High-Tech Crime*. Florencia: Cybex. 64. Available from: https://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/contributions/libro_aeec_en.pdf [Accessed 29 November 2019].
21. *Loi Relative à L'informatique, aux Fichiers et aux Libertés* (No. 78-17 du 6 Janvier 1978). Available from: https://www.cnil.fr/fr/la-loi-informatique-et-libertes [Accessed 29 November 2019].
22. Osula, A.-M., Zoetekouw, M. (2017). The Notification Requirement in Transborder Remote Search and Seizure: Domestic and International Law Perspectives. *Masaryk U.J.L. & Tech.* No. 11 (1) 103: 109. Available from: https://doi.org/10.5817/MUJLT2017-1-6 [Accessed 29 November 2019].
23. *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters of 7 April 2018.* COM/2018/225 final – 2018/0108 (COD). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN [Accessed 12 January 2020].
24. Repšs, A., Znotina, I. (2011). Electronic Evidence in Latvia: A General Overview. *Digital Evidence and Electronic Signature Law Review*, 8, 60–69. Available from: https://sas-space.sas.ac.uk/5459/1/1955-2773-1-SM.pdf [Accessed 12 January 2020].
25. *Telekommunikationsgesetz, 22 Juni 2004.* (2004). (BGBl. I, S. 1190), das durch Artikel 4 Absatz 108 des Gesetzes vom 7. August 2013 (BGBl. I, S. 3154). Available from: https://www.gesetze-im-internet.de/tkg_2004/BJNR119000004.html [Accessed 29 November 2019].
26. Vaciago, G., Silva Ramalho, D. (2016). Online Searches and Online Surveillance: the Use of Trojans and Other Types of Malware as Means of Obtaining Evidence in Criminal Proceedings. *Digital Evidence and Electronic Signature Law Review*, 13, 88–96. Available from: http://journals.sas.ac.uk/deeslr/article/viewFile/2299/2252 [Accessed 29 November 2019].