RESPONSIBILITY FOR CRIMES IN THE COMPUTER INFORMATION FIELD IN THE RUSSIAN, GERMAN AND FRENCH LEGISLATIONS

Mariya Talan, Ramil Gayfutdinov,
Kazan Federal University
gayfutdinov.r@yandex.ru

Abstract. In work the criminal precepts of law providing responsibility for computer crimes in narrow sense of this concept i.e. for crimes in the sphere of computer information are considered. As it appeared, such dual approach to definition of computer crimes is inherent not only in the Russian criminal and legal science, but also is fair in the comparative and legal analysis of the foreign legislation. We tried to show it. Responsibility for crimes in the sphere of computer information in the Russian Federation is provided by the Art. of Art. 272, 273, 274 and 274^1 The Criminal Code of the Russian Federation, in Germany - §§ 202a, 202b, 202c the Criminal code of the Federal German Republic, in France these are Art. 323-1, 323-2, 323-3, 323-3-1, 323-4, 323-4-1, 323-5, 323-6 of the Criminal code of the French Republic. Foreign criminal and legal legislations are of considerable interest to researches and their comparison to the criminal law of the Russian Federation. The purpose of such comparison is an opportunity to adopt experience of these countries. Let's note that for offers of implementation of various norms, it is necessary to pay attention to law-enforcement practice, social and economic features of this or that country and to consider a practical opportunity**.**

Keywords: computer crimes, computer fraud, cybercrimes, high-tech crimes, cyber-enabled crime, Russia, Germany, France.

INTRODUCTION.

For the first time criminal liability for crimes against safety of computer information (crime in the sphere of computer information) found the reflection in chapter 28 of the Criminal Code of the Russian Federation of 1996 (further - the Criminal Code of the Russian Federation) Introduction of criminal liability for illegal acts in the considered sphere was caused by a scientific and technological revolution, the subsequent to it information and technological modernization of the enterprises and institutions not only in Russia, but also in many developed foreign countries [1] and also emergence of world information space. Let's make a reservation that in the works we do not identify a concept "crimes in the sphere of computer information" and "computer crimes". The first term much already the second (and equivalent with it "cybercrimes", "hi-tech crimes" [2]) is also its component, including acts, responsibility for which is provided by Art. 272 "Illegal access to computer information, Art. 273 "Creation, use and distribution of malicious computer applications" and Art. 274 "Creation, use and distribution of malicious computer applications".

Since 26.07.2017 chapter 28 of the Criminal Code of the Russian Federation is added with new structure, it is necessary enhancing criminal liability for illegal impact on critical information infrastructure of the Russian Federation (Art. 274^1 Criminal Code of the Russian Federation "Illegal impact on critical information infrastructure of the Russian Federation"). *Critical information infrastructure* is formed *by* information systems, information and telecommunication networks, automated control systems of public authorities, public institutions, Russian legal entities and (or) individual entrepreneurs which on the property right, rent or on other legal ground belong the information systems, information and telecommunication networks, automated control systems functioning in health sector, sciences, transport, communication, power, the bank sphere and other spheres of the financial market, fuel and energy complex in the field of atomic energy, defensive, space-rocket, mining, metallurgical and chemical industry, the Russian legal entities and (or) individual entrepreneurs who provide interaction of the specified systems or networks and also the networks of telecommunication used for the organization of interaction of such objects. Thus, crime in the form of illegal impact on critical information infrastructure by definition is somewhat similar to a foreign concept of cyberterrorism. So in 2002 US Center for Strategic and International Studies defined cyberterrorism as "The use of computer network tools to shut down critical national infrastructure (such as energy, transportation, government operations) or to coerce or intimidate a government or civilian population (Lewis, 2002)" [3].

Attention to fight against computer crime is paid as at the international level what regularly held international scientific and practical forums and meetings [4] devoted to highly specialized subject testify to; adoption of the international agreements directed to fight against computer crimes [5]; creation at the interstate and state level of specialized bodies for fight against computer crime [6]; so, naturally, counteracts computer crime also criminal legislations of foreign countries.

Methods.

Criminal laws of foreign countries provide responsibility for various infringement of safety of computer information. The comparative and legal method of studying of the criminal legislation of the foreign states assumes their analysis in system. As such system we offer consideration of the most developed European countries with similar domestic

legal system - the Roman-German legal family. It is well-known that the most actively computer crime is shown in the countries with developed economy and breakthrough technologies. Without belittling high development of many European countries, we will limit ourselves to the analysis of two countries: The Federal Republic of Germany (further - Germany) and the French Republic.

1 Results and discussion

3.1. *The criminal legislation of the Federal Republic of Germany* consists of the Basic law (Constitution) of Germany of 1949, the Criminal code (Criminal code) of Germany of 1871 (further - CC Germany), federal criminal laws, the criminal legislation of lands and the foreign criminal legislation [7]. As main types of punishments of CC Germany provides a fine (§ 40) and lifelong or temporary imprisonment (§ 38). An auxiliary view of punishment is the ban of driving (§ 44).

CC Germany recognizes as penal criminal encroachments with use of the computer equipment. The special section on crimes against safety of computer information in CC Germany is absent [8]. In the German criminal law similar crimes on object of criminal legal protection are in two sections CC Germany - it is the Fifteenth section "Violation of Personal Privacy and Private Secrets" (§§ 202a, 202b, 202c) and the Twenty seventh section "All-dangerous Criminal Actions" (§§ 303a, 303b).

In the German criminal and legal doctrine there are also two main points of view of understanding of computer crimes according to which in narrow sense they are understood as all crimes which commission is obviously possible only by means of the computer equipment (§§ 202a, 202b, 202c, 303a, 303b), and in wide - traditional crimes, or in other words postponed from real life in virtual [9]. As computer crimes which commission is obviously possible only by means of the computer equipment the following corpora delicti in CC Germany are: ferreting out of data (§202a), interception of data (§202b), preparation for ferreting out and interception of data (§202c), located in the XV section "Violation of Personal Privacy and Private Secrets"; change of data (§303a) and computer sabotage (§303b), located in the XXVII section "Damage of Things".

In a broad sense it is possible to refer the following corpora delicti to other computer crimes: violation of confidentiality of a word, especially personal area of private life by means of shooting of images, the mysteries of correspondence, private secrets, a post and telecommunication secret, use of others secrets (§§ 201, 201a, 202, 203, 204, 206) located in the XV section "Violation of Personal Privacy and Private Secrets"; a fake of technical records (§268), a forgery of data, significant for proof (§269, §270), concealment of documents (§274), located in the XXIII section "Forgery"; creation of a hindrance for work of telecommunication installations (§317), located in the XXVIII section "All-dangerous Criminal Actions"; fraud (§263), computer fraud (§263a), abuse of check and credit cards (§266b), located in the XXII section "Fraud and Breach of Confidence"; and other crimes located in other sections of the Special part of CC Germany, e.g., distribution of pornographic materials (§§ 184 and a trace.), the materials showing violence (§ 131), insult (§§ 184 and a trace.), illegal prosecution (§ 238) and so forth and also in "additional criminal law", for example, violation of inviolability of secret information (§§ 3, 43, 44 Laws of Germany on protection of personal data, the Law of Germany on counteraction of unfair competition), illegal listening (§§ 89, 148 Laws of Germany on telecommunication), copyright infringement (§§ 106, 108, 108b the Law of Germany on protection of copyright) and so forth [10]

Due to the ratification of Germany of the Convention of the Council of Europe, computer fraud is recognized criminal action (§263a CC Germany). As CC FRG[11] of a form of realization of the objective party specified in § 263a act as ways of achievement of the mercenary purpose, the computer is used by the subject of crime as means of commission of crime [12]. CC Germany does not connect computer fraud with withdrawal and (or) the address of property. Sufficient sign is causing damage.

The institute of plurality of crimes is also familiar to the criminal legislation of Germany. According to §53 CC Germany is possible qualification of criminal actions with use of the computer equipment on set with other crimes. At the same time such acts encroaching on property are completely covered by corpus delicti §263a (computer fraud) that gives constructive completeness to norm, unlike the corpus delicti provided by Art. 159^{6} CRIMINAL CODE OF THE RUSSIAN FEDERATION.

It is remarkable that are understood by the German legislation as data such which are stored or transferred by the electronic, magnetic or other *directly not perceived person* in the ways. Thus, in CC Germany other, in our opinion, more perfect approach to definition of computer information unlike the domestic legislation.

The norm on computer sabotage (§ 303b) provides responsibility for considerable violation of data processing, having essential value for other person. The qualifying sign of computer sabotage is existence of a special subject to encroachment - essential value of data processing for foreign enterprise, corporation or public authority (paragraph 2 § 303b).

In CC Germany there is no allocation of creation, use and distribution of malicious computer applications, violations of the rules of operation of means of storage, processing or transfer of computer information and information and telecommunication networks as separate corpora delicti. Such actions are penal §§ 202a, 202b, 303a, 303b.

3.2. *The criminal legislation of the French Republic* consists of the Constitution of France 1958, international legal acts, the Criminal code of France, other codified laws, not codified criminal laws and bylaws. In UK of France all criminal actions are grouped in subject to encroachment in independent sections taking into account the value of this or that protected benefit. Distinctive feature of the criminal legislation of France is the regulation of responsibility of legal entities (Art. 121-2). UK of France provides responsibility for commission of computer crimes in the Book II establishing responsibility for crimes and offenses against the personality; To the Book III regulating responsibility for property crimes and offenses; and in the Book IV containing regulations on criminal liability for crimes and offenses against the nation, the state and public tranquility [13].

A.G. Volevodz carries out division of computer crimes on UK of France on crimes against safety of computer information, crime in information computer space and other crimes in the computer sphere which, in our opinion, is expedient for adding taking into account the changes made to the criminal legislation of France [14]. Thus, on UK of France it is possible to refer a number of the corpora delicti located in its various heads and sections to computer crimes. It is interception, plunder, use or the bringing to publicity the message ˇ, reflected by means of a long-distance communication (Art. 226-15); implementation or return of the instruction on implementation of the automated processing of inundated data without implementation of the formalities (Art. 226-16) provided in the law; implementation or return of the instruction on implementation of processing of these data without acceptance of all measures of the precautions necessary to ensure data security (Art. 226-17); collecting and data processing in the illegal way (Art. 226-18); input or storage in computer memory of the data (Art. 226-19) forbidden by the law; storage of certain data over the term (Art. 226-20) established by the law; use of data with other purpose, than it was provided (Art. 226-21); to lead the disclosure of data able to the consequences (Art. 226-22) specified in the law; acts, connected by both production and distribution on telecommunication networks of a child pornography (Art. 227-23); illegal access to the automated system of data processing or illegal stay (Art. 323-1) in it; hindrance to work or violation of work of computer system (Art. 323-2); input fraudulently in the system of information and also change or destruction contained in the automated system of data (Art. 323-3); use of the received data in office activity for commission of the crimes provided by the Art. of Art. 323-1 on 323-3 (323-3-1); special forms of partnership in the crimes provided by the Art. of Art. 323-1 and 323-1-1 (323-4 and 323-4-1); additional responsibility of natural persons for commission of the acts provided by the Art. of the Art. with 323-1 on 323-3-1 (323-5); responsibility of corporations for crimes, the provided Art. of the Art. with 323-1 on 323-3-1 (323-6); collecting or transfer contained in computer memory or a card file of information to the foreign state, destruction, plunder, withdrawal or copying of the data having character of the secrets of national defense which are contained in computer memory or in card files and also acquaintance with these data of strangers (the Art. of Art. 411-7, 411-8, 413-9, 413-10, 413-11); destruction, damage or plunder of any document, the equipment, construction, the equipment, installation, the device, technical device or the system of the automated data processing or entering of defects (Art. 411-9) into them; the acts of terrorism connected with acts in the field of informatics (Art. 421-1).

Against safety of computer information among the corpora delicti called above located in UK of France we can carry to crimes only the Art. of Art. 323-1, 323-2, 323-3, 323-3-1, 323-4, 323-4-1, 323-5, 323-6 located in Chapter III "Infringement of the systems of the automated data processing". The attention is drawn by the criminal legal protection *of the state systems of processing of personal data* which is shown in the qualified signs of the considered corpora delicti (the Art. of Art. 323-1, 323-2, 323-3 and 323-4-1).

The way of the description of the objective party of rape as the introduction the victim in contact with the performer of criminal acts thanks to telecommunication networks as a result of distribution of the messages addressed to an uncertain circle of people [15] is of a certain interest. Thus, the French legislator imposed criminal liability for mailing of a certain type of spam.

2 SUMMARY

Thus, in the sphere of a regulation of responsibility for computer crimes the brevity of statement of the objective party of corpus delicti is peculiar to the criminal legislation of Germany, in other words ways of commission of acts in details are not concretized and also there is no qualified responsibility of special subjects of crimes. The computer crimes in their narrow sense provided by CC of Germany in the majority can be committed both with direct, and with indirect intent.

The criminal legislation of France contains a wide list of ways of commission of crime and their detailed regulation, provides the high sizes of penalties and also sets responsibility of legal entities. If the criminal legislation of Germany provides the sanction sizes, insignificant in comparison, in the form of imprisonment (2-3 years), then UK of France resolves this issue to almost identically Russian - responsibility up to 5-7 years of imprisonment depending on concrete crime is provided. Besides, criminal laws of both France, and Germany provided rather severe penalties which can be estimated in tens of thousands of euro. There are significant differences in the recognized degree of public danger of computer offenses and in ways of the description of signs of corpora delicti.

As it appeared, dual approach to definition of computer crimes (in narrow and broad sense) it is inherent not only the Russian criminal and legal science, but also is fair in the comparative and legal analysis and the foreign legislation.

Conclusions

Foreign criminal and legal legislations are of considerable interest to researches and their comparison to the criminal law of the Russian Federation. The purpose of such comparison is an opportunity to adopt experience of these countries. Let's note that for offers of implementation of these or those norms, it is necessary to pay attention to law-enforcement practice, social and economic to features and to consider a practical opportunity. Therefore one of the possible further directions for researches is the judicial statistics and jurisprudence of foreign countries. Such statistics and practice is open for foreign researchers in Russian-speaking network "Internet". For example, the Portal of legal statistics of the Prosecutor General's Office of the Russian Federation (http://crimestat.ru) and the official site of Judicial department at the Supreme Court of the Russian Federation (http://www.cdep.ru/index.php?id=79) to a certain extent allow satisfying the interests.

Acknowledgements

The work is performed according to the Russian Government Program of Competitive Growth of Kazan Federal University**.**

References

1. F. Sampson, 'Cyberspace: The new frontier for policing?', Cyber Crime and Cyber Terrorism Investigator's Handbook, Chapter 1, pp. 1-2.
2. D. Wall, "Cybercrimes: New Wine, No bottles?", Invisible Crimes, Chapter 5, P. Davies et al. (eds), 1999, pp. 105-106.
3. E. Luiijf, 'Definitions of Cyber Terrorism', Cyber Crime and Cyber Terrorism Investigator's Handbook, Chapter 2, p. 13.
4. For example, 4th Interpol-Europol of Cybercrime Conference (on September 28-30, 2016, Singapore); IFIP SEC 2016 Gent, Belgium; International Conference of Cyber Security, July 25-28, 2016; Third Annual Journal of Law and Cyber Warfare Conference No. November 2016; The Law and Policy of Cybersecurity, February 5, 2016 | Rockville, Maryland, USA, etc.
5. E.g., the Convention of the Council of Europe on crime in the sphere of computer information: ETS No. 185, 23.11.2001, Budapest; the item "h" p.1 Conventions of the UN against transnational organized crime: it is accepted by the resolution 55/25 of the General Assembly of November 15, 2000; Creation of global culture of cyber security: The resolution, is adopted by the General Assembly 31.01.2003.
6. E.g., Cyber Division at FBI Headquarters USA, Departmment "K" of BSTM Ministry of Internal Affairs of the Russian Federation, Interpol.
7. Criminal law of foreign countries. The general and Special speak rapidly: the textbook for masters / under the editorship of N.E. Krylova. 4 ed. rev. and add. M.: Yurayt, 2015. Page 407.
8. See in more detail: Golovnenkov P. V. Criminal code (Criminal code) of the Federal Republic of Germany. 2nd ed. Rev. and comp. M.: Avenue, 2014. Page 24.
9. See: Golovnenkov P. Computer crime in Germany and the system of delicti//Crimes in the sphere of economy: Russian and European experience: materials VI of a joint Russian-German round table, Moscow, October 23, 2014 / edit..: A.I. Rarog, T.G. Ponyatovskaya. M, 2015. Page 28-29.
10. See: Golovnenkov P. Decree. Page 34; Weisser B. Cyber Crime. The information Society and Related Crimes. Section No. 2. Special Part. National Report o№ Germany//Electronic Review of the International Association of Penal Law. Preparatory Colloquium Section II. Moscow (Russia), 24-27 April, 2013. Criminal Law. Special Part//URL: http://www.penal.org/sites/default/files/files/RM-8.pdf (date of the address: 13.06.18).
11. Strafgesetzbuch//URL: http://www.gesetze-im-internet.de/bundesrecht/stgb/gesamt.pdf (date of the address: 13.06.18).
12. See: Hilyuta V. V. Criminal liability for plunders with use of the computer equipment//the Magazine of Russian law. 2014 No. 3 (207) of Page 114; Oryol N.A. Foreign experience of counteraction of computer crime (problem of criminalization and punishability)//Collection of scientific works of the international conference "Information Technologies and Safety". Issue 1. Kiev, 2003. Page 110-118.
13. Criminal Code of the French Republic//URL: https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719 (date of the address: 13.06.18).
14. See: Volevodz A. G. Criminal legislation on responsibility for computer crimes: experience of the different countries / A.G. Volevodz, D.A. Volevodz//Legal questions of communication. 2004. No. 1. Page 43-44.
15. See: Criminal law of foreign countries. The general and Special speak rapidly: the textbook for masters / under the editorship of N.E. Krylova. 4 ed. rev. and add. M.: Yurayt, 2015. Page 299.