Journal of Internet Banking and Commerce

An open access Internet journal (http://www.icommercecentral.com)

Journal of Internet Banking and Commerce, April 2016, vol. 21, no. S3

Special Issue: Finance, Services Sector and Commerce: Innovations and Investments
Edited By: Mihail N. Dudin

Crimes against Information Security: International Legal Aspects of Fighting and Experience of Some States

MARINA ALEKSANDROVNA EFREMOVA

Ulyanovsk State University, L. Tolstogo Street, Ulyanovsk, 432017, Russian Federation, Tel: +7(8422)41-06-79;

Email: **seamaid63@gmail.com**

PAVEL VALERIEVICH AGAPOV

Academy of the Prosecutor General's Office of the Russian Federation, 2-ya Zvenigorodskaya Street, 123022, Moscow, Russian Federation

Abstract

This article is devoted to the study of foreign criminal law providing for liability for information security offences. The relevance of that problem is driven by the intensifying IT development and globalization, under which both information security of a separate state and international information security may not be achieved by the efforts of a single state. Efforts need to be consolidated, and a uniform approach to the solution of that matter needs to be worked out. The author stresses that in the Russian Federation and in most foreign countries there is no systematic approach to criminal law protection of information security except for the Republic of Poland. In most foreign criminal codes

(CC), the provisions on information security protection are spread all over Special parts. In most foreign countries, offences against confidentiality of professional and official secrets are criminalized, while in the Civil Code of the RF such provisions are missing. Meantime, foreign criminal law does not specify separate elements of crimes in order to protect tax secrets. Criminal law protection of state secret is solved differently in foreign countries: via detailed regulation for state secret offences and under totally missing respective provisions in CC. Regarding cybercrime, the CIS countries used to apply the uniform approach to criminalization of respective elements of crime as criminal laws of most of them adopted the provisions of Model Criminal Code of the CIS member states. However, in future, due to the amendments of articles providing for liability for cybercrime that approach was lost. In foreign countries, along with the traditional illegal access to computer information, the liability is provided for computer sabotage, computer fraud. The author opines that a systematic approach is required to criminal law protection both in the Russian Federation and in foreign countries. Only uniform, joint, consolidated acts may efficiently serve to fight information security offences.

Keywords: I**nformation; Information Security; Secret; Information Resource; Computerized Information; Criminal law**

INTRODUCTION

Rapid development of information and communication technologies today is reflected in virtually all spheres of personal, public and state life. Globalization and information society development in most foreign countries, the coming integration into the global information society require from states to solve the new task – ensuring information security and prevention of information-related crimes. Russia follows the wide approach to the information security, which includes both IT and social/humanitarian, political/ideological aspects [1,2]. The solution of information security problem surely may not be achieved by the efforts of a single state, so great role is played by international cooperation and international regulations. Extremely important is the uniform approach to international information security, cyberterrorism, information weapon, information wars, etc. In that connection, special relevance and importance is gained by comparative research of laws, based on which some scientifically reasonable offers on the improvement of both national and international laws may be made.

METHODOLOGY

Comparative research method enables to find not only differences but succession features and similarities of various legal systems related to various historical types and legal families as well as to formulate general theoretical provisions and structures, find the dependencies of operation and development accounting for the specifics of legal systems of various countries.

Meantime, systematic approach to understanding of information security as an object of

criminal offence enables to fully and totally analyze the criminal law provisions of various countries and move offers on their optimization and unification.

RESULTS

Currently at the international level there is no regulation governing the issues of criminal law protection of information security, but also there is no uniform understanding of information security, its basic threats, and possible joint steps to prevent and fight them. To solve the issues of ensuring part of information security – cybersecurity – the European Convention on Cybercrime 2001 was adopted [3]. Adoption of that Convention is a culmination of a great work. For the four years preceding its adoption some 27 drafts were submitted. The final version dated May 25, 2001 contained preamble and four chapters. It was submitted to European Commission on fighting cybercrime at the 50th plenary meeting on June 18-22, 2001.

That Convention in the initial version divided cybercrimes into four groups (later, upon the adoption of extra protocol, the number of groups grew to five). The first group included cybercrimes, i.e., crimes against confidentiality, integrity and accessibility of computer data and systems. They are, in particular, illegal access, illicit interception, interference in data, interference in system, etc.

The second group included the crimes in connection with the use of computers. They are forgery with the use of computer technologies, fraud for illicit economic personal benefit or benefit of third parties.

The third group includes crimes in connection with content. First of all, it is child pornography, and Convention in detail explains which acts on distribution of child pornography should be prosecuted (making, offering or making available for use, distribution, transfer, purchase, owning).

The fourth group includes crimes in connection with copyright. Those crimes are not specified in the Convention: classification of such crimes relates to the competence of national legislatures.

In early 2002, Protocol was adopted to the Convention, adding to the list of cybercrimes distribution via information and communication technologies of racist or other information, incitement to violence, hatred or discrimination of any person or a group of persons based on racial, national, religious or ethnic background.

As opined by both Russian and foreign researchers, the classification of crimes in the Convention is not total or final as cybercrimes are changing as time goes even more than the other kinds of crimes. With the invention and public implementation of new information and communication technologies, with the shift of the existing public relations to the cyberspace that list will need to be updated. Besides, some provisions of the Convention ignore the fundamental principle – respect of state sovereignty. That

was the reason why the Russian Federation and a number of other states did not ratify the Convention.

Russia opines that currently the need to develop a new universal document is urgent to replace the European Convention on Cybercrime 2001. Russia's position is that such convention should be developed within the UN. That will allow, on one hand, to maximally account for the concern of all countries, and on the other hand, to make the document really global, without which cybercrime fighting may not be efficient enough. Thus, Russian initiatives currently cover on the whole range of threats in the information sphere. It means that international regulations are urgent for creating safe and reliable digital infrastructure. Security Council of the RF jointly with the Ministry of External Affairs developed the draft Convention on international information security [4]. It has a wider sphere of use as distinct from the European Council's Convention. The draft Convention developed by Russia is aimed to govern the acts of states to ensure information security. Article 10 of the draft Convention reads that member states exert efforts to criminalize the use of information resources and/or affecting them in information space for illicit purposes including illegal disclosure, breach of confidentiality, integrity and availability of information, taking legislative and other steps required to provide for and apply the liability for attempt, accompliceship and commitment of criminalized socially dangerous acts in information space.

Despite numerous positive moments, that draft Convention has not been supported by other states yet.

The authors suggest that the need has escalated for adoption of a new international regulation the enforcement of which would guarantee peaceful application of information and communication technologies for the benefit of national development and international stability. In this regulation, crimes against information security should be classified and recommendations should be provided for states in connection with criminalization of acts against information security in the national legislatures. Adoption of such a regulation will become a pledge of efficient fighting against information security on various levels.

Efficient international cooperation in that area should follow the study and analysis of foreign regulations which will enable to create scientifically reasonable offers on the improvement of the national criminal regulations of the RF, account for them in the course of legislative activity and on the other hand will save foreign legislators from making mistakes.

DISCUSSION

It is thought that information security from the point of view of the criminal law should be considered as a system of public relations including: public relations ensuring the realization of the right to information and protection of information from illicit access; public relations ensuring security of information resources; public relations ensuring

safe use of information and communication technologies. In the criminal law of the Russian Federation the liability is provided for offences of even some elements of information security. Therefore, as authors opine, to ensure information security in the Russian Federation, the CC of the RF should contain a separate section Crimes against information security covering on corpus delicti in which information security is the basic object of the offense.

Comparative legal research shows that criminal regulations of foreign countries are also characterized mainly by the absence of systematic approach to criminal law protection of information security. However, in some countries the information protected by law is specified as a sort or type. So, the CC of the Republic of Poland [5] contains Chapter XXXIII called Crimes against information protection including articles making liable for breach of confidentiality of state secret; illicit acts regarding professional and official secret; breach of secrecy of correspondence; offences against significant information; illicit acts regarding information recorded on computer data storage device including information on national security, safe communications, governmental administration, other state authority or municipal authority, failure or inability to automatically collect or transfer such information.

Separate chapter covers on offences against secret information in the CC of the Republic of Korea [6], chapter XXXV called Crimes related to breach of secrecy. It provides for the liability for disclosure of professional secrecy and breach of secrecy of communication.

Offences against professional and/or official secrecy are criminalized in criminal laws of a great number of foreign countries. For example, the Penal Code of Estonia [7] contains Article 157 Breach of the liability to keep confidential secrets related to professional or official activity, in compliance with which a person shall be liable for disclosing information about health, private life or commercial activity of another person if he/she has to keep such information secret by law and such information became known in the course of professional or official activity.

In the Russian Federation there are no special regulations setting the liability for breach of confidentiality of the said kinds of secrets. Although scientists announced the notions on including them in the CC of the RF, it should be noted that in the Russian Federation there are no federal acts on professional secret and official secret, so including those criminal elements in the CC of the RF will lead to confusion. Those regulations presumably should be blanket meaning the need to apply to the relevant provisions of laws. Today, the qualification of disclosure of professional or official secrets is possibly under various articles of Special part of the CC of the RF and depends on the nature of information and the subject of disclosure. First of all, those are articles 137, 138, 155, i.e., the crime elements related to confidentiality of information being personal or family secret, secrecy of communication, secrecy of child adoption. In most countries of post-Soviet area like in the Russian Federation the said crime elements are traditionally included in chapters/sections on crimes against civil constitutional rights. Such

approach is seen in the CC of Republic of Armenia [8] in chapter 19 Crimes against constitutional rights and freedoms of a man and a citizen; in section 5 of the Ukrainian CC Crimes against electoral, labor and other personal rights of a man and a citizen [9]. An interesting approach was used by the German legislator. The Criminal Procedures of the Federative Republic of Germany [10] in section 15 Violation of privacy and private secrecy, article 203 provide for liability for breach of private secrets, i.e., disclosure of secrets related to private life or production or commercial secret, which was shared with or otherwise became known to a person in the course of activities. Thus, the German legislator provided for criminal liability for disclosing professional and official secret as derivatives from private secrets as professional secrets are based on private secrets protected from disclosure by legal restrictions for those who were entrusted with secrets when required [11,12].

The French CC uses the term intimacy of private life [13], breach of which may be in the form of interception, recording or unconsented transfer of confidentially expressed words; fixing, recording or transfer of image of a person being in a private place without his/her consent. Also, making the said words or person's image public or permissiveness in that connection is also punished.

Right to privacy of communication or correspondence, mail, telegraph and other messages, serving as a component of right to private life is also protected by foreign criminal law. However, some differences may be found here. The Belgian legislature classified breach of communication or telephone communication secrecy as crimes against public order [14]. The Spanish CC [15] does not contain any special provision on breach of that secret. Article 197 of Spain's CC is devoted to the protection of private life in general while criminal liability is provided for collecting and disclosing any information without owner's consent contained in letters, e-mails, information from data, electronic or television storages, archives and the use of technical devices for those purposes. Articles 198 and 199 are linked with article 197 and they cover on cases when crime subjects are governmental officials and persons who knew others' secrets due to professional activity. From the point of view of legal technique, Estonian legislator's method deserves some attention, as article 156 of Penal Code Breach of communication secrecy did not specify communication means transferring messages and expressed part 1 very briefly yet laconically: Breach of correspondence secrecy and messages transferred via communication means. In Criminal Procedures of the Federative Republic of Germany the liability for breach of correspondence secrecy and breach of mail and communication secrecy is differentiated. Breach of correspondence secrecy means opening sealed letter or any other sealed written document not addressed to that person or getting to know the content of such written document without opening it by the use of technical means. Breach of mail and communication secrecy is the transfer of information about facts being mail or telecommunication secrets by an owner or a worker of a corporation professionally engaged in mail or telecommunications service or opening by those persons of messages sealed and handed to them.

In most foreign countries, illicit acts regarding the information being commercial or bank

secrets are criminal. Meantime, collecting the information related to that kind of secrets in a few countries is classified as industrial or commercial espionage. For example, article 254 of the Belarus Republic CC [16] provides for liability for commercial espionage, i.e. stealing or illicit collecting of information being commercial or bank secrets for the purpose of disclosure or illegal use. The Austrian CC [17] also provides for the liability for breach of commercial or industrial secret, investigating commercial or industrial secrets. Meantime, investigating any commercial or industrial secret for a foreign country is considered a more dangerous crime. In Russia, the liability for receiving and disclosing the information being commercial, tax or bank secrets is provided for in article 183 of the CC. It should be noted that foreign criminal legislature covers on commercial and bank secrecy while in the Russian Federation the said article includes tax secrets as well. It must be said that commercial, bank and tax secrets have various legal nature. Tax secret is covered fully by official and professional secret concept and does not need criminal law protection independently.

Criminal liability for disclosure of state secret is provided for in different ways in foreign criminal law. For example, Austria's CC contains a special section providing for the liability for deliberate disclosure of state secrets (article 252), breach of state secret (article 253) and investigating state secret (article 254). The Criminal Code of Austria defines state secret in article 255. It means information, items or knowledge, including written materials, drawings, models and messages about things which are known to a limited number of persons and must be kept secret from foreign authorities, supranational or interstate entities to prevent the danger of causing material damage to the defense of the Austrian Republic or relations of the Austrian Republic with foreign authorities or supranational or interstate entities. The criminal law of the FRG approaches the state secret protection in greater detail compared to the CC of Austria. The CC of the FRG contains five articles on state secret offence. They are espionage (article 94), disclosure of state secret (article 95), taking possession of state secret for the purpose of disclosure or breach of state secret (article 96), espionage agency activity (article 98). Article 97a of the FRG Criminal Procedures provides for liability for disclosure of illegal secrets – information about violations of free democracy or facts of violations of interstate agreements on arms control kept secret from the FRG's partners. State secret, like in Austria, is defined in the criminal law. According to article 93 of the CC of the FRG, it is facts, items or information available to a limited number of persons only which must be kept secret from foreign authorities for the purpose to prevent the danger of causing material damage to the external security of the Federative Republic of Germany.

The Criminal Code of France, as distinct from others, neither contains any definition of state secret nor uses that term at all. Instead of that, the French legislator uses the term national defense secrets. According to part 1, article 413-9 of the French CC, national defense secrets are: information, technologies, items, documents, data and files related to the national defense and being the objects of protective measures preventing their disclosure. They may include other information if its disclosure may cause damage to the national defense or breach any secret of the national defense. The procedure of

classifying information as related to the national defense is set forth by a special decree of State Council.

The criminal law of Spain, like that of France, does not contain state secret term but in the Spanish CC there is the term secret and information related to the national defense. The said information has the following features: it is defined as closed and secret; it is able to cause damage to the national defense. Offences against it may be expressed as: investigating, forgery, spoilage, disclosure of secret information.

In the Russian Federation, state secret term is defined in article 2 of the RF Act No. 5485-1 dated 21.07.1993 On state secret [18], as information protected by government regarding its military, foreign policy, economic, intelligence, counterintelligence and operational investigations activity distribution of which may cause damage to the security of the Russian Federation. In the CC of the RF, in turn, the articles 275 Treason, 276 Espionage, 283 Disclosure of state secret, 283.1 Illicit receipt of information being state secret, 284 Loss of documents containing state secret do not contain any material differences compared to their foreign analogues.

In the end of the last century most develop countries saw a negative social phenomenon called cybercrime. Initially, along with the occurrence of crimes in computer information sphere, foreign legislature began developing in two directions: wider interpretation of traditional regulations; development of specialized regulations on cybercrime [5, p. 8]. In that connection, the matter of criminalization of illicit acts against computer information was solved in the foreign legislature rather differently. The criminal law of the CIS is uniform in general regarding criminalization of offences against computer information, in many of them the provisions of Model Criminal Code of the CIS countries [19] were adopted, but some of them have already undergone some changes. For example, the Criminal Code of Azerbaijan Republic [12] contains chapter 30 Cybercrimes. Earlier, it was called Crimes in computer information sphere. Article 271 of that chapter provides for criminal liability for illicit access to computer systems. In notes to that article, the key terms are defined, including computer system which means any device or a group of interconnected devices engaged in automated data processing using relevant software. Computer information means any information (facts, data, software and notions) suitable for use and processing in a computer system. Besides that, chapter 30 of the Azerbaijan CC provides for the liability for: illicit possession of computer information (article 272); illicit interfering in computer system or computer information (article 273); distribution of means made for committing cybercrimes (article 273-1); counterfeiting computer data (article 273-2). Regarding counterfeiting computer data, it means unconsented deliberate input, change, deletion or blocking computer data for the purpose of passing them off as authentic (true) computer data or using them. The new CC of Republic of Kazakhstan effective since January 2015 contains chapter 7 Criminal offences in information technologies and communications, even its name may be admitted good. The above chapter includes 9 articles: article 205. Illicit access to information system or information communications network; article 206. Illicit deletion or modification of information; article 207. Deliberate impair of operation of

information system or information communications network; article 208. Illicit taking possession of information; article 209. Forcing to transfer information; article 210. Making, use or distribution of malware and malware products; article 211. Illicit distribution of limited access electronic information resources; article 212. Providing services for hosting Internet resources pursuing illicit purposes; article 213. Illicit change of identification code of mobile communication subscriber's device, subscriber identification device and making, use, distribution of software changing identification code of subscriber's device [20].

In the course of the foreign law analysis, there was seen the lack of uniform approach to the description of the elements of illicit access to computer information liable in the Russian Federation according to article 272 of the CC. As the subject of this crime, computer data are admitted in some countries. For example, clause "a" of article 202 of the Criminal Procedures of the FRG provides for criminal liability for illicit receipt by a person of data for himself/herself or any other person, which were not assigned for him/her and were under special protection from illegal access. Article 202 contains a special note that it covers on data, stored or transferred via any electronic, magnetic means or otherwise, not perceived directly. Clause "b" of article 202 included in the Criminal Procedures in 2007 provides for liability for illicit receipt of data by an unauthorized person using technical means for himself/herself or any other person in the course of their nonpublic transfer via telecommunications (telephone, fax, teletype) and computer communication (e-mail) regardless from the form and coding of those data, if any. Article 186-1 of the CC of France provides for criminal liability for illicit interception of data in telecommunication systems. In compliance with the first part of article 323, a crime shall be unauthorized access to automated system of data processing or part of such system if in the result of such access the data contained in such system were deleted or changed or system's operation was impaired. The second part of that article provides for liability for interfering in the operation or impairing the operation of automated data processing system. The third part of article 323 is devoted to the change of data in systems for the purpose of forgery or fraud. From the analysis of regulations above we may conclude that the criminal law covers on the protection of data and telecommunication systems.

In general, in most foreign countries, along with offences against data confidentiality, the liability was provided for committing crimes like unauthorized break in computers and computer networks; computer sabotage; computer fraud.

Conclusion: The above analysis enables to conclude that only in the criminal law of Poland a systematic approach to criminal law protection of information security may be seen. In a number of foreign states, some various kinds of secrets are protected systematically. In general, in most countries, likewise in Russia, the provisions on the liability for offences against information security are spread all over Special part of the criminal law. It is suggested that international cooperation, in turn, will not ensure any results without the development of agreed and uniform approaches to fighting information crimes. States yet will have to find a consensus on what is information

security as an object of criminal law protection. Different understanding of that issue, limited to merely technical or computer aspects complicates taking relevant steps, so further scientific development of that issue is required.

REFERENCES

1. Zinovieva YS (2013) International Information Security. Moscow: MGIMO-University.

2. Mazurov VA (2002) Computer Crimes: Classification and Fighting Methods. Moscow: Paleotip.

3. (2001) Convention of the European Council on Cybercrime. Date Views. 26.11.2015 www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/185.

4. (2011) Convention on International Information Security (Draft). Date Views 26.11.2015. www.scrf.gov.ru/documents/6/112.html.

5. Kuznetsova NF, Lukashov AI (2001) Criminal Code of the Republic of Poland. St. Petersburg: Yuridicheskiy Tsentr Press.

6. Republic of Korea: Criminal Code (1953) Date Views 26.11.2015. www.refworld.org/docid/3f49e3ed4.html.

7. Criminal (Penal) Code of Estonia (2002) Date Views 26.11.2015. http://www.legaltext.ee/text/en/X30068K8.htm

8. Criminal Code of the Republic of Armenia (2002) Date Views 26.11.2015. www.parliament.am/legislation.php?sel=show&ID=1349&lang=rus.

9. Criminal Code of Ukraine (2001) Date Views 26.11.2015. zakon1.rada.gov.ua/laws/show/2341-14.

10. Golovnenkov PV (2014) Criminal Procedures (Code) of the Federative Republic of Germany. Moscow: Prospekt.

11. Petrukhin IL (1998) Personal Secrets (Man and Authorities). Moscow: Institute of State and Law.

12. Criminal Code of Azerbaijan Republic (1999) Date Views 26.11.2015. http://www.constcourt.gov.az/laws/32

13. Golovko LV (2002) Criminal Code of France. St. Petersburg: Yuridicheskiy Tsentr Press.

14. Matsnev NI (2004) Criminal Code of Belgium. St. Petersburg: Yuridicheskiy

Tsentr Press.

15. Kuznetsova NF, Reshetnikov FM (1998) Criminal Code of Spain. Moscow: Zertsalo.

16. Criminal Code of the Republic of Belarus (1999) Date Views 26.11.2015. http://etalonline.by/?type=text&regnum=HK9900275.

17. Serebrennikova AV (2001) Criminal Code of Austria. Moscow: IKD Zertsalo-M.

18. (1993) Act of the Russian Federation No. 5485-1 “On State Secret” (1993, July 21).

19. Model Criminal Code of the CIS Member States (1996) Adopted by the Resolution of Interparliamentary Assembly of the CIS Member States.

20. Criminal Code of Kazakhstan Republic (2014) Date Views 26.11.2015. online.zakon.kz/Document/?doc_id=31575252#pos=335;-247&sel_link=1004096288.