European Proceedings of
Social and Behavioural Sciences
EpSBS

www.europeanproceedings.com

e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2020.10.05.345

SCTMG 2020

International Scientific Conference «Social and Cultural Transformations in the Context of Modern Globalism»

CYBERCRIME PREVENTION: COMPARATIVE ANALYSIS OF CRIMINAL LAWS OF AZERBAIJAN, RUSSIAN AND ARMENIA

Vorobiev Victor Victorovich (a)*, Gracheva Yulia Victorovna (b), Ilyin Igor Vyacheslavovich (c), Malikov Sergey Vladimirovich (d), Kapinosov Erik Olegovich (e)
*Corresponding author

(a) Syktyvkar State University, Syktyvkar, 64-13, Pushkina Str., Syktyvkar, Russia, vorobvv@gmail.com
(b) Kutafin Moscow State Law University, 11-285, Ostrovityanova Str., Moscow, Russia, uvgracheva@mail.ru
(c) Nizhny Novgorod Academy of the MVD of Russia, 1-10, Sadovaya Str., Sokolskoe Settlement, Nizhny Novgorod oblast, Russia, igor_ilyin@mail.ru
(d) Kutafin Moscow State Law University Mozhaysk Freeway, 112a - 111, Odintsovo, Moscow oblast, Russia, s.v.malikov@yandex.ru
(e) Ministry of Internal Affairs for the Republic of Komi, 25-62, Svobody Str., Syktyvkar, Russia, eric.kapinosov@yandex.ru

Abstract

Crime in the IT field has a stable trend for growth and it concerns the essential spheres of activities of individual countries as well as the global community as a whole. Due to that, improving the legislation to prevent and counteract this type of criminal infringements is a pressing issue. Analysis, logical and rather-legal analysis revealed that there are significant differences in the criminal legislations of Azerbaijan, Russia and Armenia in the area of counteracting the computer crime. Among the differences are: differing lists of computer-related crimes, differing content of similarly named components of crime, lack of legal interpretation of some terms that are present in articles; specific features in qualification of certain crimes; certain inconformity between the criminal law of the countries and the model criminal law of the Commonwealth of Independent States' participants. Criminal statistics data that the authors give for cybercrime in Russia for the period from 2016 to 2018 support the conclusions of certain problems in this field of law enforcement. Synthesis, generalization and analogy used as cognitive methods allowed revealing a number of similar as well as specific characteristics of criminal laws of Azerbaijan, Russia and Armenia; some of the differences are quite significant. Some of these differences are provided with the authors' evaluation that will allow legislator to improve the criminal legislation in question in the future. Materials of this paper may be useful to legislators, legal experts, law enforcement officers, criminal judges, professors and students of law.

Keywords: Cybercrime, criminal liability, information security.

https://doi.org/10.15405/epsbs.2020.10.05.345
Corresponding Author: Vorobiev Victor Victorovich
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

Development of information technologies gave rise to a new criminal phenomenon – cybercrime. Appearance of new types of crime requires constant improvement of not only software and hardware countermeasures, but also of laws in the field of counteracting the cybercrime.

2. Problem Statement

Currently, due to globalization, there is a necessity to improve international and national legislations, as there are serious drawbacks in both international and national law that inhibit efficient prevention of such crimes.

3. Research Questions

The subject of research is criminal law standards on cybercrime liability in Azerbaijan, Russia and Armenia.

4. Purpose of the Study

The research objective is to conduct a rather-legal analysis of articles in the criminal codes of Azerbaijan, Russia and Armenia with the view of subsequently formulating proposals for improvement of these laws for better harmonization between themselves and with international treaties

5. Research Methods

The paper uses such cognitive methods as synthesis, generalization, analogy and rather-legal analysis.

6. Findings

Development and active introduction of computer technologies create a wide area for criminal activities in the field of digital technologies. According to analytical data from executive committee of the Commonwealth of Independent States, about 70% of CIS population are able to connect to the Internet. Among the CIS states, the Russian Federation experienced the largest number of computer attacks; Russia hit the Top 10 for this indicator, together with such countries as the USA, China, South Korea, Hong Kong, the United Kingdom.

We assume that one of the most important factors that inhibits prevention of cybercrime is a lack of common approaches in the international cooperation for counteracting this criminal phenomenon, which is on the rise globally (de Hert, Parlar, & Sajfert, 2018; Tosoni, 2018).

In 2019, the International Telecommunication Union under the UN published a report titled Global Cybersecurity Index. According to the report, Russia takes the 28th position in the global cybersecurity rating. Of CIS countries, Kazakhstan took the 42nd place, Uzbekistan, Moldova, Ukraine and Azerbaijan took 55th, 56th, 57th and 58th position, respectively. Belarus was 74th, while Armenia was 84th. The

https://doi.org/10.15405/epsbs.2020.10.05.345
Corresponding Author: Vorobiev Victor Victorovich
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

lowest position among the CIS countries is taken by Kyrgyzstan at the 129 place. The top five consists of the United Kingdom, the United States, France, Lithuania and Estonia. In the general rating, Europe is the leader in implementation of cybersecurity regulations and countermeasures against cybercrimes and spam (GCI, 2018).

Previously, Russia took higher positions in the Global Cybersecurity Index: in 2017 it was 10th position (GCI, 2017), while in 2014 it was 12th position (GCI, 2014).

Today, we may note that all the CIS countries include cybercrime-related liabilities in their criminal codes. At that, all the 11 criminal codes (of 11 participating countries) provide separate chapters where the rules covering liabilities for IT crimes are collected. They have various titles and may have serious differences between themselves, however, there are also some similarities.

Republic of Azerbaijan. Chapter 30, Cybercrimes, which is in the Section X, Crimes against public safety and public order of the Criminal Code of the Republic of Azerbaijan contains the following Articles: 271 (Unauthorized access to computer system); 272 (Unauthorized abstraction of computer information); 273 (Unauthorized intervention into computer system or computer information); 273-1 (Circulation of means produced to commit cybercrime); 273-2 (Forgery of computer data) (Criminal code of the republic of Azerbaijan, 2019).

Unauthorized access to computer system in Article 271 of the Criminal code of Azerbaijan is understood as a deliberate access to a computer system or a part of it by a person who has no access rights or with infringement of access rights, or with the aim of abstracting computer information or with other personal interest.

Disposition of this article construct the body of the crime as formal and the crime is considered committed at the moment of entering the computer system, independent of consequences if any.

It should be noted, that the Criminal Code of the Rupublic of Azerbaijan criminalizes unauthorized access to a computer system, and not to computer information, thus significantly expanding applicability of the criminal law in comparison with the corresponding legislation of other CIS countries.

Note to the Article 271 states that “computer information” shall be understood as any information suitable to processing in a computer system.

Such an approach to defining the concept of computer information may be welcomed and taken into consideration in legislation of other countries, including Russia.

The next body of crime is unauthorized abstraction of computer information. Within the Article 272 it is explicated as deliberate acquisition of computer information transmitted in a computer system, including by reading electromagnetic radiation, when the information is not intended for public use and the deed is performed by a person having no rights to abstract the information with the help of technical means.

Part 1 of the Article 273 covers liabilities for unauthorized deliberate damage, destruction, corruption or blocking of computer information if such act resulted in significant damages.

Liability for causing serious obstacles to operation of a computer system by means of unauthorized influence on computer information is covered in Part 2 of the Article 273.

Significant damages here are damages exceeding one thousand manats or causing other significant damage to legally protected interests.

https://doi.org/10.15405/epsbs.2020.10.05.345
Corresponding Author: Vorobiev Victor Victorovich
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

Serious obstacles to operation of a computer system are understood as such a disturbance to the operation of the computer system when the owner's or user's abilities to use the system are significantly limited, including information exchange with other computer systems.

Thus, analysis of the above bodies of crime witness to division of complex crimes into separate crimes such as: Unauthorized access to a computer system, unauthorized abstraction of computer information, unauthorized influence on information. Such approach seems quite reasonable.

A separate item is the body of crime covered by Article 273.1 that provides liability for Circulation of means produced to commit cybercrime. This crime is divided into three types that are fixed in different parts of the regulation.

The first part provides liability for production, acquisition, sale, transportation, distribution or use of devices or computer software intended for commission of cybercrime if it resulted in significant damages.

The second part of the Article 273-1 provides criminal liability for production, storage or acquisition of passwords, access codes and other data allowing for unauthorized access to computer information if it resulted in significant damages.

Sales, distribution or creation of other conditions for acquisition of computer passwords with the aim of committing a cybercrime are covered by the Part 3 of the Article 273-1.

Thus, we may see that in the criminal legislation of the Republic of Azerbaijan, computer passwords, access codes and other data that allow obtaining unauthorized access to computer information are identified as the target of crime. This development may also be welcomed, as it creates legal foundation for prevention of cybercrime at its preparatory stage.

The last body of crime in the Cybercrime chapter provides liability for forgery of computer data (Article 273-2), that is, unauthorized change to, destruction or blocking of data in order to pass the forged data for valid.

Thus, cybercrime in the Criminal Code of the Republic of Azerbaijan may be conveniently divided into three groups:

1) Unauthorized access to a computer system, unauthorized abstraction of computer information, unauthorized influence on information.

2) illegal circulation of computer passwords, access codes and other data with the aim of committing cybercrime;

3) forgery of computer data.

Russian Federation In the criminal law of the Russian Federation, cybercrime is covered in Chapter 28 «Crime in the field of computer information», included in Section IX «Crime against public safety and public order» (Criminal Code of the Russian Federation, 2019). This is basically the only common feature in cybercrime-related criminal legislation between Russia and the Republic of Azerbaijan.

As presented in Chapter 28 of the Criminal Code of Russia, cybercrimes may be conveniently divided into three groups: unauthorized access to computer information protected by law (Article 272); illegal handling of harmful software (Article 273); infringement of rules of computer operation (Article 274).

https://doi.org/10.15405/epsbs.2020.10.05.345
Corresponding Author: Vorobiev Victor Victorovich
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

In 2017, this chapter was supplemented with the Article 274[1], providing liability for unauthorized influence on the essential information structure of the Russian Federation. The authors do not identify this body of crime as a separate type of cybercrime, as information in the essential information structure may be equated with the computer information protected by law, while the methods of unauthorized, destructive influence onto it bear no significant difference from those given above.

Liability for unauthorized access to computer information takes place only with respect to computer information protected by law, e.g., official or commercial secret, secret of private life and other information that is protected by the law of the Russian Federation.

In contrast to the Criminal Code of the Republic of Azerbaijan, criminal liability for unauthorized access according to the Criminal Code of the Russian Federation takes place only in cases where information was destroyed, blocked, modified or copied. Thus, the fact of of familiarizing oneself with information without destructive influence or copying has no criminal consequences.

Republic of Armenia. Chapter 24 of the Criminal Code of the Republic of Armenia is titled «Crimes against security of computer information». Thus, we may see that in Armenia there is a peculiar approach to definition of computer crime.

The stated chapter contains seven bodies of crime providing for liability for crimes against security of computer information: Unauthorized access to (entering) a computer information system (Article 251); changing computer information (Article 252); computer sabotage (Article 253); unauthorized abstraction of computer information, access to computer information (Article 254); production or sale of special means for unauthorized access (Article 255); development, use and distribution of harmful software (Article 256); infringement of operational rules of a computer system or network (Article 257) (Criminal code of the Republic of Armenia, 2019).

This list includes a crime, which is absent from the criminal laws of Russia and Azerbaijan, namely, computer sabotage (Article 253).

Computer sabotage is understood as destruction, blocking, corruption of computer information (software) or computer hardware, or damage to computers or information media. This experience may also be deemed positive.

The Article 251 provides liability for unauthorized access (entering) to computer information protected by law, committed with breaking a protection system and due to negligence resulted in harmful consequences for the information, computer system or network, or in other significant damages.

Negligence as a form of guilt may cause some questions. However, on careful examination of other bodies of crime in the same chapter it becomes evident that presence of deliberate guilt in case of unauthorized influence on computer information or hardware resulting from unauthorized access shall lead to liability under different bodies of crime in Chapter 24 of the Criminal Code of the Republic of Armenia, e.g., 252, 253, 254.

Liability for changing computer information or provision of invariably false information to a computer is provided by Article 252. A mandatory condition for applicability of this article is significant damages without attributes of embezzlement, which allows separating these crimes from embezzlements committed with the help of computer technologies (Article 181). Unfortunately, regulations of this chapter lack the statement of a sum that shall be considered significant damages; in other articles where

https://doi.org/10.15405/epsbs.2020.10.05.345
Corresponding Author: Vorobiev Victor Victorovich
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

such sum is set there are no references to the cybercrime-related articles. We assume that enforcer shall apply analogy here.

Unauthorized abstraction of computer information (Article 254) is understood as unlawful copying or other acquisition of information, including by interception of communication channels.

Here, one may note a difference form Article 272 of the Criminal Code of the Russian Federation, where definition of the computer information is provided in the comment. There, it is stated that computer information is represented in a form of electric signals, independent of means of storage, processing and transmission. In Russian scholarly literature one may find critical rhetoric against this definition of computer information. There is a position that fixation of the term "computer information" in such a way is impractical. To support their critical position, such authors usually reference lack of similar regulatory definitions in all the Criminal Codes of CIS countries and in many European Codes (Fatyanov, 2017).

The second part of the Article 254 provides criminal liability for coercion to transfer computer information on pain of disclosure of some information that the person affected would like to keep secret, or under the risk of violence or damage to property of the person affected or those close to them.

This regulation is not very common for cybercrime, as it pertains more to crime against person. Similar clauses are present in the Article 209 of the Criminal Code of the Republic of Kazakhstan (coercion to transfer of information) and Part 2 of Article 301 of the Criminal Code of the Republic of Tajikistan (unlawful abstraction of computer information).

Similarly, Article 273-1 of the Criminal Code of Azerbaijan and Article 255 of the Criminal Code of Armenia point to unlawful production or sale of special software and hardware means for unauthorized access to (entering) the protected computer information. Despite the necessity to include such an article into the Criminal Code of Russia, there is currently no information on any such plans. To a certain degree, within the framework of the criminal law of the Russian Federation, such circulation of unlawful means may be qualified under Article 273 (unlawful handling of harmful software).

However, Armenian legislators separated creation, application and distribution of harmful software including viruses for unlawful influence on or copying of computer information, or distribution of media with such software as a separate crime under the Article 256.

Not all criminal legislations of CIS countries followed this lead and installed separate regulations for unlawful circulation of harmful software into their codes. For instance, such regulations are absent from the Criminal Codes of the Republic of Azerbaijan and the Republic of Moldova. In these countries criminal activities related to harmful software are covered by the articles that provide liability for creating software or hardware for commission of cybercrime (Article 260 of the Criminal Code of the Republic of Moldova and Article 273.1 of the Criminal Code of the Republic of Azerbaijan). At the same time, majority of CIS countries include such regulations in their criminal law.

Concluding this chapter is the Article 257 of the Criminal Code of the Republic of Armenia that provides liability for infringement of rules of operation of computers. This activity is deemed a crime if it is committed by a person with access to the computer and the activity resulted in destruction, blocking or modification of information, or computer malfunction or other significant damages.

https://doi.org/10.15405/epsbs.2020.10.05.345
Corresponding Author: Vorobiev Victor Victorovich
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

This type of cybercrime is not included into some criminal codes of the CIS countries. Similar bodies of crime are present in the criminal codes of Russia (Article 274), Belarus (Article 355), Moldova (Article 261), Ukraine (Article 363), Uzbekistan (Article 278-1), Tajikistan (Article 304).

It should be noted, that in the Russian Federation this body of crime is almost useless and legal statistics shows the number of persons annually brought to justice for this crime in single digits (in 2016 there were 2 such persons, in 2017 – no, while in 2018 only 1 person was brought to justice under the Article 274 of the Criminal Code of Russia) (9). Such a low efficiency of the criminal regulation is due to ambiguity in interpreting the term "rules of operations". Russian law lacks a regulation explaining what shall be understood as rules of operation of the processing means of computer information and what directives are to be included with them (The data of judicial statistics, 2019).

7. Conclusion

Criminal codes of Azerbaijan, Russia and Armenia have significant differences that encumber international cooperation between these countries in counteraction and prevention of cybercrime. Besides, is should be noted that some discussed regulations might be adopted by other CIS countries as successful practices.

References

Criminal code of the Republic of Armenia. (2019). Retrieved from http://www.parliament.am/legislation.php?ID=1349&sel=show&lang=rus

Criminal code of the republic of Azerbaijan. (2019). Retrieved from https://online.zakon.kz/m/document/?doc_id=30420353

Criminal code of the Russian Federation. (2019). Retrieved from http://www.consultant.ru/document/cons_doc_LAW_10699

De Hert, P., Parlar, C., & Sajfert, J. (2018). The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law. *Comput. Law & Security Rev., 34*(2), 327–336. https://doi.org/10.1016/j.clsr.2018.01.003

Fatyanov, A. (2017). On the definition of "computer information" in Russian criminal legislation. *Inform. Law, 3*, 11–16.

Global Cybersecurity Index (GCI). (2014). Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2014.aspx

Global Cybersecurity Index (GCI). (2017). Retrieved from https://www.itu.int/pub/D-STR-GCI.01-2017

Global Cybersecurity Index (GCI). (2018). Retrieved from https://www.itu.int/pub/D-STR-GCI.01-2018

The data of judicial statistics. (2019). Retrieved from http://www.cdep.ru/index.php?id=79

Tosoni, L. (2018). Rethinking Privacy in the Council of Europe's Convention on Cybercrime. *Comput. Law & Security Rev., 34*(6), 1197-1214. https://doi.org/10.1016/j.clsr.2018.08.004