Computer Crimes in Criminal Legislation of the Russian Federation and the State of Texas (USA)

Alexey Fatyanov[1], Maria Grigorieva[2], Taulan Boziev[3], Sergey Polyakov[4], and Anna Skachko[5]
[1]Plekhanov Russian University of Economics, Moscow, Russia
[2]Plekhanov Russian University of Economics, Moscow, Russia
[3]State Institute of Economics, Finance, Law and Technology, Gatchina, Russia; St. Petersburg State University of the Interior Ministry of Russia, St. Petersburg, Russia
[4]Novosibirsk State Technical University (NSTU), Novosibirsk, Russia
[5]Krasnodar University of the Ministry of Internal Affairs of Russia, Krasnodar, Russia

Summary
The main purpose of the article is to compare approaches to the legal regulation of liability for computer crimes in Russia and in the state of Texas (USA). Some explanations are given to the terms and definitions of concepts that are analyzed and compared (for example, "criminal liability" or "computer crimes", "corpus delicti"). Next, the assessing the differences and similarities between Russian and Texas legislation is done. One of the first points that attracts attention is that the Texas Criminal Code classifies computer crimes as a general category of crimes against property. In Russia, this group of criminally punishable acts is classified as crimes against public safety and public order. Unlike the Criminal Code of Texas, where a broad glossary of definitions of various concepts is presented, such concepts are rare in the Criminal Code of the Russian Federation. For example, Russian law does not contain the concept of "computer" at the level of federal law, so it would be useful to study this category from the Texas Criminal Code. The next part of the article examines and compares certain types. In particular, it is concluded that the approach of the Texas legislator is broader and more rational. For example, when considering cases of illegal access to legally protected computer information, the law enforcement officer and the court should prove only two facts: the fact of knowingly gaining access and the fact that there is no valid consent of the owner of the computer, computer network or computer system. In the Russian model, it is much more complicated. In the final part of the article, a comparative analysis of penalties in criminal law, their types and features is carried out.

Keywords:
criminal law, criminal offense, misconduct, computer, computer crimes, the Criminal Code of the Russian Federation, Texas legislation, digital economy.

1. Introduction

This topic is rather relevant for a number of reasons. First of all, due to the need to develop Russian legislation on the digital economy in general, as well as the concept of computer crimes in particular. In order to satisfy all participants in legal relations, it is necessary to study the positive and negative foreign experience. After all, this is the only way to avoid unwanted mistakes. In this regard, this article provides a brief analysis of some aspects of computer crimes provided for by the Criminal Code of Russia and the Criminal Code of Texas (USA) [1, 2]. Also, for comparative legal purposes, the main similarities and differences of doctrinal and legal approaches to the assessment of certain concepts in legal science are analyzed.

2. Materials and Methods

The main research method in this case was the Comparative Legal Method, which made it possible to study foreign legal acts and experience. For example, it showed that the Texas legislator's approach to defining the subjective and objective side of crimes is broader and more rational than the Russian one. The law enforcement officials and the court should prove only two facts: the fact of knowingly gaining access and the fact that there is no valid consent of the owner of the computer, computer network or computer system. This method also made it possible to form the author's position that the approaches of the Russian criminal law and the criminal law of the state of Texas in relation to determining access to protected information are in many respects similar [3]. However, the Texas legislator's approach more broadly protects the rights of owners of computers, computer networks, and systems. In general, thanks to this comparative method, it can be stated that the sanctions for the considered computer crimes in Russia and the state of Texas are comparable.
It also became clear that the Russian approach has a certain advantage in relation to illegal actions involving the use of malicious computer programs, since it extends criminal law to a much wider range of malicious software, and not just to ransom ware.

And, finally, the comparative method made it possible to draw attention to two types of criminal offenses that are absent in the criminal legislation of the Russian Federation, but their introduction into it would be desirable - these are: "Interaction with an electronic voting machine" and "online impersonation".

Manuscript received June 5, 2022
Manuscript revised June 20, 2022
https://doi.org/10.22937/IJCSNS.2022.22.6.79

The systematic scientific approach made it possible to initially consider the complete picture of criminal law and then compare the individual elements of this system - computer crimes.
The historical method made it possible to consider two national legislation taking into account historical factors associated with the formation of special features of legal families. Thus, comparisons became possible due to the historical fact that Texas adopted the civil law system due to colonial influence.

Through the use of methods of analysis, real information was obtained about the effectiveness of the application of some norms in Russia, which made it possible to talk about their hypothetical improvement, taking into account foreign experience.

3. Results Analysis

The idea of this small study was dictated primarily by the fact that we are currently witnessing a real boom in the development of information technologies. Each of the developed countries, as well as the world as a whole, are entering a new stage - the period of building the so-called "digital" economy [4], where the possibilities of telecommunication systems and networks are becoming one of the main foundations of economic relations.
This trend will inevitably lead to an increase in the number and variety of socially dangerous offenses, to which states must respond [5], including by establishing various types of legal liability. Taking into account the factor that this work is focused primarily on the foreign reader, the authors considered it necessary to make small comments and clarifications on what certain legal constructions are in the Russian Federation.

So, legal liability of the punitive type in Russia has two varieties: the usual criminal liability, which will be discussed in this work, and administrative liability. The latter type has also been codified (there is a Russian-wide Code of Administrative Offenses, as well as similar codes in most constituent entities of the Russian Federation), however, the system and procedure for applying legal sanctions when bringing to administrative responsibility has been significantly changed towards simplification.

Let's return, however, to criminal responsibility. Why did we choose Texas criminal law as a model for our comparative study? The choice was due to the fact that the system for determining the punishable acts in it is similar to the Russian one. That is, there is a single codified act containing a list of descriptions of acts and sanctions. It is well known that in the United States criminal law is the prerogative of each of the states and in the Russian Federation it is a single law for the entire state. According to the Russian legal tradition, any legislative acts establishing or eliminating criminal liability must be implemented into this act by making appropriate changes to it.

One of the first points that should be discussed is that the Texas Penal Code classifies computer crimes as a more general category of crimes against property. In Russia, this group of criminally punishable acts is classified as crimes against public safety and public order. Also does not coincide with the Penal Code of Texas ("Computer Crimes") and the title of the corresponding section - in the Criminal Code of the Russian Federation it is called "Crimes against Computer Information". This is due to the influence on the criminal legislation of other branches of Russian law - in this case, information law, which deals with the definition of various categories of information in the interests of legislative regulation.

Unlike the Penal Code of Texas, where a wide glossary of definitions of various concepts used in describing punishable acts is presented, in the Criminal Code of the Russian Federation such concepts are mainly either described directly in the text of the norm, or are given in the notes to the relevant articles. But latter is more an exception then the rule. Thus, the notes to the first article of the section under consideration indicate that "computer information is understood as information (messages, data) presented in the form of electrical signals, regardless of the means of their production, processing and transmission" [6]. From the point of view of technical sciences, the definition is somewhat clumsy, but so far we are using it. The rest of the concepts, such as "computer network", "computer program", "computer system", in determining the punishable acts are borrowed from other legislative acts regulating relations in the information sphere.

Paradoxically, but in Russian law at the level of federal law (this type of laws regulates the main part of relations in the information sphere in accordance with the division of legislative competence between the Russian Federation and its subjects) [7], there is no concept of "computer", so we were happy to analyze this category from the Penal Code of Texas and recognize it as quite comprehensive, taking into account the maximum possible options for the construction and purpose of such devices (a computer according to the Penal Code of Texas means "electronic, magnetic, optical, electrochemical, or other high-speed data processing device that performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, or communication facilities that are connected or related to the device" [8]. In our further analyzes within the framework of this work, we will proceed from it.
The second definition, which we would like to focus on, is the content of the category "critical infrastructure facility". In the Russian Federation, a special legislative act has been adopted that regulates relations in a similar area, referred to as the Federal Law of July 26, 2017, No. 187-FZ "On the Security of the Critical Information Infrastructure of the

Russian Federation", however, it operates with more general concepts, while The Texas Penal Code lists specific types of objects, illegal actions against information systems of which are punishable. These include: intake structure, water treatment facility, wastewater treatment plant, or pump station; a chemical manufacturing facility; a refinery; an electrical power generating facility, substation, switching station, electrical control center, or electrical transmission or distribution facility; a natural gas transmission compressor station; a liquid natural gas terminal or storage facility; a telecommunications central switching office; a port, railroad switching yard, trucking terminal, or other freight transportation facility; a gas processing plant, including a plant used in the processing, treatment, or fractionation of natural gas; a transmission facility used by a federally licensed radio or television station" [8]. As it seems to the authors of this work, this approach, due to its specificity, is more acceptable for real law enforcement.

Let's move on to considering some articles of the Texas Penal Code in comparison with the Criminal Code of the Russian Federation, describing specific punishable acts. Here we would like to clarify that we do not intend to consider all crimes and misdemeanors without exception included in Chapter 33 "Computer Crimes" of the Penal Code of Texas, since some of them are included in other sections of The Special Part in the Criminal Code of the Russian Federation, but we focus on computer crimes, which are interpreted in a similar way in Chapter 28 of the Criminal Code of the Russian Federation "Crimes in the field of computer information" due to the fact that it is more effective to conduct a comparative analysis.

Here we would also like to draw attention of American reader to one of the important points of Russian criminal law as a branch of legal science, namely, the existence of a formal legal structure "*corpus delicti*", which Russian scientists and practical lawyers are used to use to describe criminal offenses. This legal structure consists of four elements: the object, the objective side, the subject, the subjective side. According to the prevailing scientific views, the object of a crime is understood as a group of public relations, which is harmed by a specific illegal act included in the criminal law, the objective side is a description of a specific criminal act, the subject is a natural person capable of bearing criminal responsibility, and the subjective side is a description of goals and motives by which an individual was guided during committing a punishable act, as well as a form of guilt (intent or negligence). In this case, in order, first of all, to save the attention of readers and space on the pages of a scientific publication, we will analyze mainly the objective side of the act, as well as the sanctions for its commission.

Clause 33.02 "Breach of computer security" of the Penal Code of Texas describes in clause "a" the objective side of the punishable act as follows: "A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner" [8]. From the point of view of Russian criminal law, this is a deliberate crime. A negligent act in this case is not punished.

The closest to this act is the description of the punishable act given in the first part of Article 272 "Unlawful access to computer information" of the Criminal Code of the Russian Federation, where it is interpreted as follows: "Unlawful access to legally protected computer information, if this act entailed the destruction, blocking, modification or copying of computer information" [9].

We can point out that the Texas legislator's approach is broader and more rational. The court should prove only two facts: the fact of knowingly gaining access and the fact that there is no valid consent of the owner of the computer, computer network or computer system.

In the Russian model, everything is much more complicated. First, it is necessary to detect computer information protected by law. Most authoritative commentators of the Russian Criminal Code agree that computer information protected by law is information with limited access (state, commercial secrets, personal information of citizens or objects of copyright and related rights) [10]. Secondly, it is necessary to recognize access to computer information as illegal. The concept of unauthorized access in the Russian regulatory framework at the present time is contained in the Methodological Recommendations for the Prosecutor's Supervision over the Execution of Laws in the Investigation of Crimes in the Field of Computer Information, approved by the General Prosecutor's Office of the Russian Federation (a non-regulatory act). According to these Recommendations, "access to confidential information or information constituting a state secret by a person who does not have the necessary powers (without the consent of the owner or his legal representative) is considered illegal, provided that special means of its protection are provided" [11]. Although the Texas Penal Code does not explicitly state this, it should be assumed that access to protected information, and not to computer information in general, is punished, which brings the approaches of Russian criminal law and the criminal law of the state of Texas closer together.

Further, in order to bring an individual to criminal liability in the Russian Federation it is also necessary that the result of unauthorized access is the destruction, blocking, modification or copying of computer information. If one of these facts is not proven, then the *corpus delicti* is not formed.

Which approach can be considered more correct? The authors of this work believe that both approaches have a right to exist. The Russian approach builds more conventionalities, including for the purpose of the so-called "economy of criminal repression", that is, to bring to justice only in case of actual damage to the legitimate interests of

the legitimate owner of computer information. The Texas legislator's approach more broadly protects the rights of owners of computers, computer networks and systems.

Now let's discuss the punishments. A crime without aggravating circumstances, mentioned above, is punished under the Texas Penal Code as a class B offense (misdemeanor). For its commission 180 days of imprisonment and a fine of US $ 2,000 are provided [8].

The Criminal Code of the Russian Federation contains a wider range of possible punishments applied on an alternative basis. These include: a fine of up to 200,000 rubles or in the amount of the wages or other income of the convicted person for a period of up to eighteen months; correctional labor for up to 1 year; restriction of freedom for up to 2 years; forced labor for up to 2 years; imprisonment for up to 2 years [9]. The presence of a large number of alternative sanctions is due to modern trends in the criminal legislation of Russia towards its humanization, which is expressed, among other things, in the possibility of an individual approach of the court when imposing punishment and the reasons that made him commit a crime. This crime in Russia belongs to the category of crimes of small gravity, the lowest level of hierarchy.

The authors also do not want to judge which of the approaches is more acceptable. It depends on a number of factors, including the specific socio-political or crime situation in Russia and the state of Texas. We only note that the very fact of criminal prosecution in Russia, regardless of the size of the sanction, entails quite a lot of negative consequences for citizens, especially in the field of further employment, which is an additional reason to refrain from illegal behavior.

In general, we can state that the sanctions for the above acts in Russia and the state of Texas are comparable.

More significant differences between the Criminal Code of the Russian Federation and the Penal Code of Texas are seen with the additional qualification of the above-described acts. At the same time, a much more complex classification is used in the Penal Code of Texas than in the Criminal Code of the Russian Federation. Subsection b-1 of clause 33.02 of the Texas Penal Code would be referred to in Russian criminal law as a "*qualified corpus delicti*", that is, an act with a greater level of public danger. In this clause, the Texas legislator rather scrupulously describes such a group of acts, establishing the following:

"A person commits an offense if, with the intent to defraud or harm another or alter, damage, or delete property, the person knowingly accesses:

(1) a computer, computer network, or computer system without the effective consent of the owner; or

(2) a computer, computer network, or computer system:

(A) that is owned by:

(i) the government; or

(ii) a business or other commercial entity engaged in a business activity;

(B) in violation of:

(i) a clear and conspicuous prohibition by the owner of the computer, computer network, or computer system; or

(ii) a contractual agreement to which the person has expressly agreed; and

(C) with the intent to obtain or use a file, data, or proprietary information stored in the computer, network, or system to defraud or harm another or alter, damage, or delete property.

(b-2) An offense under Subsection (b-1) is:

(1) a Class C misdemeanor if the aggregate amount involved is less than $100;

(2) a Class B misdemeanor if the aggregate amount involved is $100 or more but less than $750;

(3) a Class A misdemeanor if the aggregate amount involved is $750 or more but less than $2,500;

(4) a state jail felony if the aggregate amount involved is $2,500 or more but less than $30,000;

(5) a felony of the third degree if the aggregate amount involved is $30,000 or more but less than $150,000;

(6) a felony of the second degree if:

(A) the aggregate amount involved is $150,000 or more but less than $300,000;

(B) the aggregate amount involved is any amount less than $300,000 and the computer, computer network, or computer system is owned by the government or a critical infrastructure facility; or

(C) the actor obtains the identifying information of another by accessing only one computer, computer network, or computer system; or

(7) a felony of the first degree if:

(A) the aggregate amount involved is $300,000 or more; or

(B) the actor obtains the identifying information of another by accessing more than one computer, computer network, or computer system" [8].

Consistently, the sanctions are as follows: for the smallest offense (misdemeanor of class C), the convicted person receives a fine in the amount of $ 500, for the most significant - a first degree felony - the convicted person receives a sentence of imprisonment for a term of 5 to 99 years, or life imprisonment and a $ 10,000 fine.

In the Russian Federation, the punishment for "*qualified (aggravated) corpus delicti*" is almost never graded in such detail. Usually these are three to four additional levels. In article 272 of the Criminal Code of the Russian Federation, which we compare with clause 33.02 of the Penal Code of Texas, the gradation has three additional levels:

- the same act that caused major damage (defined by the Criminal Code of the Russian Federation in the amount of 1,000,000 rubles or more) or committed out of selfish interest (punishable by a fine in the amount of 100,000 to 300,000 thousand rubles or in the amount of the convicted person's salary or other income for a period from one year

to two years, or correctional labor for a period of 1 to 4 years, or imprisonment for the same period);
- the same acts committed by a group of persons by prior conspiracy, or by an organized group or by a person using his official position (punishable by a fine of up to 500,000 rubles or in the amount of the convicted person's salary or other income for a period of up to 3 years with the deprivation of the right to hold certain positions or engage in certain activities for up to 3 years, or restraint of liberty for up to 4 years, or forced labor for up to 5 years, or imprisonment for the same period);
- the same acts, if they entailed grave consequences or created a threat of their occurrence are punishable by imprisonment for up to seven years [9].

As we can see, in this case, there is a clear approach, in which the sanctions of the Russian criminal law look much more modest in comparison with the sanctions of the Texas Penal Code. This is explained by the fact that, according to the established Russian legislative tradition, the most punishable in terms of the magnitude of the sanction are a number of crimes against the life and health of citizens and a number of crimes against state power. All other criminal sanctions are at a lower level. Also, the Russian legislator does not accept too wide discretion in terms of establishing the terms of punishment, such as from 5 to 99 years. Life imprisonment under the Criminal Code of the Russian Federation is possible only as a substitute for the death penalty, the application of which was suspended by the decision of the Constitutional Court of the Russian Federation.

The second type of criminal acts, which have some similarity between the approach of the criminal legislation of the state of Texas and the Russian Federation, is clause 33.023 "Electronic data tampering" of the Texas Penal Code. To a certain extent, it corresponds to article 273 "Creation, use and distribution of malicious computer programs" of the Criminal Code of the Russian Federation. Paragraph 33.023 deals with specific types of computer malware, or ransom ware. It is a punishable offense in which money, property or service is required to the owner to remove the identified "computer pollution or blockage" and restore access.
In the Russian version, not only the installation itself is criminally punishable, but also the creation (development), as well as the distribution in any way of computer programs and other computer information.
In the opinion of the authors of this work, in this case the Russian approach has some advantage, since it extends criminal law to a much wider range of malicious software, and not just to ransom ware.
And, finally, I would like to draw attention to two types of criminal offenses that are absent in the criminal legislation of the Russian Federation, but their introduction into it would be desirable.

The first is clause 33.05 "Tampering with direct recording electronic voting machine". According to this clause, " A person commits an offense if the person knowingly accesses a computer, computer network, computer program, computer software, or computer system that is a part of a voting system that uses direct recording electronic voting machines and by means of that access:
(1) prevents a person from lawfully casting a vote;
(2) changes a lawfully cast vote;
(3) prevents a lawfully cast vote from being counted; or
(4) causes a vote that was not lawfully cast to be counted" [8].
It is noteworthy that this crime is unambiguously referred by the legislator to grave crimes of the first degree, for which punishment is from 5 to 99 years in prison or life imprisonment.
In Russia, the system of electronic voting through computer systems is only developing, so the criminalization of this acts will be necessary in the very near future.
As e-commerce and the digital economy in general develops in the Russian Federation, it becomes relevant for us to criminalize such an act as the "online impersonation" provided for in clause 33.07 of the Texas Penal Code, that is, using the name of another person to create a web page on a commercial social network or other website on the Internet, as well as the transmission of emails, instant messages and other messages that mention the name, domain address, phone number or other element of identifying information belonging to another person without his consent with intent to harm any person.
On the contrary, the Texas Penal Code does not criminalize such a significant, from our point of view, group of acts as "violation of the rules for the operation of storage, processing or transmission of protected computer information or information and telecommunication networks and terminal equipment, as well as the rules for accessing information and telecommunication networks, that entailed the destruction, blocking, modification or copying of computer information, causing major damage "(punishment up to 2 years in prison, and with aggravating circumstances - up to 5 years in prison). In our opinion, the establishment of criminal punishment for this group of acts is quite justified, since careless actions of personnel can cause very significant harm to the interests protected by law in many areas of economic activity (for example, in the banking sector, etc.).

4. Conclusions

The result of this study was a comparison of the criminal legislation of the Russian Federation and the state of Texas (USA) in the field of computer crimes. Similarities and differences were identified, and conclusions were drawn about the possible use and implementation of some, in our opinion, useful and well-developed norms in Russian legislation.

In conclusion of this study, its authors express the hope that it has served, at least to a small extent, to broaden the understanding of the scientific circles of the state of Texas and the United States in general regarding the approaches taken in the Russian Federation concerning the criminalization of acts related to computer information, computer systems and networks, and for the scientific community of the Russian Federation - the approaches adopted in the state of Texas, USA.

References

[1] Carr, J.: *Inside Cyber Warfare: Mapping the Cyber Underworld*. Second Edition. O'Reilly Media (2011).

[2] Winmill, L.B., Metcalf, D.L., Band, M.E.: *Cybercrime: Issues and Challenges in the United States*. Digital Evidence and Electronic Signature Law Review, vol. 7 (2010). https://doi.org/10.14296/deeslr.v7i0.1921

[3] Bergman, P.J.D., Berman, S.J.D.: *The Criminal Law Handbook: Know Your Rights, Survive the System*. Sixteenth Edition. NOLO (2020).

[4] Pushkarev, V.V., Artemova, V.V., Ermakov, S.V., Alimamedov, E.N., Popenkov, A.V. Criminal Prosecution of Persons, Who Committed Criminal, Acts Using the Cryptocurrency in the Russian Federation. Revista San Gregorio, vol. 42, pp. 330-335 (2020). https://doi.org/10.36097/rsan.v1i42.1566

[5] Pushkarev, V. V., Poselskaya, L. N., Skachko, A. V., Tarasov, A. V., & Mutalieva, L. S.: Criminal Prosecution of Persons Who Have Committed Crimes in The Banking Sector. *Cuestiones Políticas*, 39(69), 395–406 (2021). https://doi.org/10.46398/cuestpol.3969.25

[6] Federal Law "*On the security of the critical information infrastructure of the Russian Federation*" dated July 26, 2017 N 187-FZ (last edition). http://www.consultant.ru/document/cons_doc_LAW_220885/

[7] Article 71 Constitution of the Russian Federation (adopted by popular vote on 12/12/1993 with amendments approved during the nationwide vote on 07/01/2020). http://www.consultant.ru/document/cons_doc_LAW_28399/7faf10d5db4889ccd421abd45b63fd2b43a3dea7/

[8] Texas Constitution and Statutes.: *Penal Code* (2022). https://statutes.capitol.texas.gov/?link=PE

[9] Article 272 of the Criminal Code of the Russian Federation. «*Illegal access to computer information*». Criminal Code of the Russian Federation of 06/13/1996 N 63-FZ (as amended on 12/30/2021). http://www.consultant.ru/document/cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/

[10] Lebedeva, V.M. (ed.): *Commentary on the Criminal Code of the Russian Federation*. In 4 volumes. Special part. Section IX (itemized). Moscow (2017).

[11] General Prosecutor's Office of the Russian Federation. *Guidelines for the implementation of prosecutorial supervision over the implementation of laws in the investigation of crimes in the field of computer information* (2013). https://epp.genproc.gov.ru/ru/web/gprf/documents/scientific-materials?item=4900252