Digital Crimes as a Contemporary Threat for Society

Spector L.A.* Bondarenko Ya.A.

Institute of Service Sector and Entrepreneurship of the Don State Technical University in Shakhty
Corresponding author: e-mail:Shpigunova96@mail.ru

ABSTRACT

The Internet has incorporated not only the virtues of globality but all the global vices as well. The power of the Web is increasingly becoming a means of committing unlawful actions. The development of telecommunications has led not only to the expansion of human capabilities but also to the emergence of negative factors that adversely affect private life in the international information network. With the rapid development of computer technology and the increasing spread of automated processing of personal data, as well as the openness of the global network, the problem of privacy and confidentiality of personal data is becoming increasingly important. Despite this, currently, you may find in the global network any information, including someone's personal data. Unlawful services for the collection and dissemination of information about individuals and legal entities are widespread. Databases of owners of apartments, land, cars, address and telephone bases, passport bases are very popular.

Keywords: *digital law, crime, information networks, Internet, criminal responsibility, statistics*

1. INTRODUCTION

The Internet has incorporated not only the virtues of globality but all the global vices as well. The power of the Web is increasingly becoming a means of committing unlawful actions. This is aggravated by the ability to inflict maximum damage with minimum costs. So according to the US FBI, the average damage from one such crime is 650 thousand US dollars. For the first time, a computer was used as a theft tool from the Bank of Minnesota in 1956. And the first law was adopted in the USA only in 1978, which provided for the responsibility for modification, destruction, or unauthorized access to computer data. The domestic first criminal case refers to the end of the 70s, and the proper legal framework appeared only in the mid-90s.

The popularity of this crime is growing due to impunity. The media also fuels interest in this type of activity, creating an atmosphere of romance and fame. The intensified hacker intrusions into various computer items show the vulnerability of computer networks, which, in an effort to simplify the exchange of information and accelerate its processing, lose their security. Hackers are attracted not only by private but also by government agencies. In 1986-1989 German hackers upon the instructions of the KGB of the USSR copied classified materials from the computer networks of the Pentagon and NASA. In recent years, the following facilities have been hacked: the website of the Russian Security Council, the website of the Federation Council, the Moscow City Telephone Network, the websites of the Federation Council, Goskomstat, the Ministry of Internal Affairs, and the Government of Moscow. Since October 2002, there has been a "hole" in the protection system, through which access to the census database is available. However, state policy in the field of ensuring user privacy is very weak, which means that the constitutional rights of citizens are not fully guaranteed. Recently, information about the leak of personal data of users of social networks and online stores is becoming more common. In 2019, personal data of Russians began to flow through IT specialists. This was reported by the Izvestia newspaper with reference to the study of the DeviceLock cybersecurity company. The company studied insider information leaks from Russian companies. Of all the reported cases, 2% of leaks occurred through system administrators. This is a new type of insider that was not recorded in previous studies. According to the representative of the company, the reason is that the profession of an IT specialist is transformed from an elite to a massive one accompanied by a decrease in earnings and requirements for applicants. According to the calculations of Oganesyan, taking into account the average salary of the system administrator in Moscow of 150 thousand rubles, selling, for example, 100 thousand pieces of information about bank customers may bring 500 thousand to 2 million rubles. Despite the fact that a new type of personal data leak in the outgoing year accounted for only 2%, it includes for more than a quarter of all leakages by volume, as the study said. The remaining 98% of cases of data leaks occurred with the help of specialists from other departments of banks and companies, including specialists from the back office and customer support. Data from more than a billion users of social networks in the world leaked to the Network. There were no passwords and bank card data in the database, however, details from

Facebook, Twitter, and LinkedIn, as well as phone numbers and email addresses of users, were stored there. A hacker discovered a file in the public domain on GoogleCloud

2. METHODOLOGICAL RESEARCH

The scientific and technological revolution entailed serious social changes, the most important of which is the emergence of a new kind of social relations and public resources, information ones. The information has become the fundamental principle of the life of modern society, as well as the subject and product of its activities, and the process of its creation, accumulation, storage, transmission, and processing, in turn, has stimulated progress in the field of tools for its production: electronic computer technology (ECT), telecommunications, and communication systems.

The appearance on the market in 1974 of compact and relatively inexpensive personal computers, with the improvement of which the boundaries between mini- and large computers began to varnish, made it possible to connect an unlimited circle of people to powerful information flows. The question about the controllability of access to information, its safety and good quality arose. Organizational measures, as well as software and hardware facilities, were not effective enough [7]. The problem of unauthorized interference is especially acute in countries with highly developed technologies and information networks. Computer information, in accordance with Article 2 of the Law “On Information, Informatization, and Information Protection,” means details about persons, items, facts, events, phenomena, and processes regardless of the form of their presentation, but with reference to commented articles, not the information itself is understood under computer information but the form of its presentation in a machine-readable form, i.e. the combination of characters recorded in computer's memory, or on a machine medium (floppy disk, optical, magneto-optical disk, magnetic tape, or another tangible medium). When considering cases, it should be borne in mind that under certain conditions, physical fields may also be information carriers [5]. The rapid quantitative increase in crime and its qualitative changes conditioned by the aggravation of contradictions in various areas of public life, the frequent reorganization of the law enforcement system, the imperfection of legislation and its frequent changes, serious omissions in law enforcement practice, accelerate the development of computer crime as a social phenomenon [6]. The lack of a clear definition of computer crime, a unified notion of the essence of this phenomenon significantly complicates the definition of the tasks of law enforcement agencies in developing a unified strategy to combat it. Computer crimes may conditionally be divided into two vast categories, crimes related to interference with the operation of computers and crimes that use computers as required technical means. We will now omit “near-computer” crimes related to programmers' copyright infringement, illegal business on computer technology, etc., as well as physical destruction of computers.

We would like to list some of the main types of crimes related to interference with computers:

1. Unauthorized access to information stored on a computer.

Unauthorized access is usually carried out using someone else’s name, changing the physical addresses of technical devices, using information left after solving problems, modifying software and information facilities, stealing information media, installing recording equipment connected to data transmission channels.

Unauthorized access may also occur as a result of a system failure. For example, if some user files remain open, it is possible to gain access to parts of the data bank that do not belong to it. Everything happens as if a bank client, having entered a room designated to it in a vault, notices that one wall of the vault is missing. In this case, he may penetrate into other people's safes and steal everything stored therein [10].

2. Introduction into the software of “logical bombs” that actuate when certain conditions are met and partially or completely disable the computer system

3. Development and spread of computer viruses

4. Criminal negligence in the development, manufacture, and operation of software and computer systems, which led to grave consequences.

The problem of negligence in the field of computer technology is akin to an imprudent fault when using any other type of equipment, transport, etc.

5. Counterfeiting computer information

The idea of a crime is to falsify the output information of computers in order to simulate the performance of large systems, of which a computer is an integral part. If a fake is rather cleverly executed, it is often possible to deliver deliberately defective products to the customer.

Forgery of information may also include juggling the results of elections, votes, referenda, etc. After all, if each voter cannot be sure that its vote is registered correctly, then the introduction of corruption in the final reports is always possible [9].

6. Theft of computer information

If ordinary theft is subject to the existing criminal law, then the problem of theft of information is much more complicated. The joke that our software is distributed only through theft and the exchange of stolen goods is not very far from the truth. In the case of improper ownership, machine information may not be removed from the funds but copied. Therefore, machine information should be highlighted as an independent subject of criminal law protection [8].

3. RESEARCH RESULTS

So, computer crimes should be understood as socially dangerous actions provided for by criminal law, in which machine information is the object of a criminal attack. In this case, machine information, a computer, a computer system, or a computer network will serve as the subject or instrument of a crime [2]. Approaching the classification of computer crimes is most reasonable from the standpoint of components of crime, which may be classified as computer crimes. Although the components of computer crimes are currently not clearly defined, a set of types of unlawful actions may be identified to be included therein. We would like to list some of the main types of crimes associated with interfering with the operation of computers: “following a fool” - physical penetration into production facilities.

“catch the tail” - an attacker connects to the communication line of a legitimate user and waits for a signal indicating the end of the work.

“computer boarding” - an attacker manually or using an automatic software picks up a code (password) for access to the computer system using a regular telephone set:

“slow choice” - the offender studies and learns the system of protection against unauthorized access, its weaknesses, identifies areas that have errors or unsuccessful logic of the software structure, program breaks (gap, hatch), and introduces additional commands that allow access;

“masquerade” - an attacker penetrates a computer system, posing as a legitimate user with its codes (passwords) and other identifying ciphers;

“bamboozlement” - an attacker creates conditions when a legitimate user communicates with an illegal terminal, being absolutely sure that it is working with the legitimate subscriber it requires.

“emergency” - an attacker creates the conditions for the occurrence of failures or other malfunctions in the operation of computer equipment. At the same time, a special program, which allows emergency access to the most valuable data, is executed. In this mode, it is possible to "disable" all the means of information protection available in the computer system.

4. DISCUSSING THE RESULTS

The Criminal Code of the Russian Federation provides for various punishments for computer crimes, as well as divides crimes into groups [1].

Confidentiality of information is expressed in the right to privacy; this is a fundamental human right that is on the same level as the right to life and freedom of conscience. There is criminal responsibility for violation of privacy In the Russian Federation. Article 137 of the Criminal Code of the Russian Federation establishes punishment for violation of privacy; Article 138 — for violation of the secrecy of communication. Article 272 of the Criminal Code of the Russian Federation establishes responsibility for unauthorized access to legally protected computer information [2, p. 294]. Moreover, a set of laws in the Russian Federation protect private information:

–Federal Law “On Information, Information Technologies, and Information Protection” No.149-FZ dated 07/27/2006

–Law of the Russian Federation “On Federal Bodies of Government Communication and Information” No. 4524-1 dated 02/19/1993.

–Federal Law “On Personal Data” No. 152-FZ dated 07/27/2006

The level of computer crime is determined largely by objective reasons and directly depends on the general level of informatization of society. Most foreign and domestic researchers note that Russia lags behind developed countries by an average of 20 years in computerization issues. If the first computer crime in the USA was recorded in 1966, then in the former USSR in 1979. Therefore, the trends in the development of computer crime in Russia may differ dramatically from those in developed countries. According to experts in this field, first of all, a significant quantitative increase in computer crimes is expected. A number of reasons contributes to it, the main of which are as follows: first, a sharp increase in unemployment and a drop in living standards among the so-called “white-collar” population against the background of the general economic crisis and the crisis of non-payments; second, mass uncontrolled computerization and the use of the up-to-date electronic means in all areas of activity, particularly, financial, banking, and credit institutions of all forms of ownership; and third, the absence of an appropriate legal framework that impedes, to any noticeable extent, the spread and suppression of computer crimes. Among the positive trends, a decrease in the number of thefts of computer equipment and peripherals may be predicted, which is due to a significant drop in their prices and relative availability, as well as a reduction in the illegal use of machine resources and machine time. At the present stage of IT development in Russia, the need has arisen for a detailed study of the issue of the fundamentals of the forensic investigation of computer crime. It should be noted that the commitment of computer crimes, as well as the commitment of any other common types of crimes, leaves “traces,” the detection, recording, and studying which is an indispensable condition in the investigation and solving of this type of crime and in the fight against "technogenic" crime in general [3]. However, state policy in the field of ensuring user privacy is very weak, which means that the constitutional rights of citizens are not fully guaranteed. Recently, information about the leak of personal data of users of social networks and online stores is becoming more common. The rapid development of cross-border computer crime has put the world community in need of establishing international cooperation and joint counteraction to computer criminals.

The First Document of the Council of Europe is Recommendation No. R89 (9) of the Committee of Ministers of the Council of Europe on Computer Crimes (September 13, 1989). The listed offenses recommended for inclusion in national law include:

– computer fraud;

– computer forgery;
– damage to computer data and software;
– computer sabotage;
– unauthorized access;
– unauthorized interception;
– unauthorized reproduction of microcircuits.

Soon, the international "Convention on Cybercrime" emerged. It contains many procedural provisions. Russia is a party to the "Agreement on Cooperation of the CIS Member States in the Fight against Crime in the Field of Computer Information."

Forms of cooperation: exchange of information, coordinated activities, training of qualified personnel, creation of information systems, and sharing legal acts [4].

The world got known about computer crimes for the first time in the early 70s when a fairly large number of such actions were revealed in America. As is known, the most dangerous crimes are those that are economic in nature. Initially, the history shows that criminal justice authorities fought it with the help of traditional rules of law on crimes against property: theft, misappropriation, fraud, breach of trust, and the like. However, the practice soon showed that this approach does not meet all the requirements of the current situation since many offenses in the field of computer activity are not covered by the traditional components of crime.

5. CONCLUSIONS

To ensure the safety of Internet users and their privacy, it is required to ensure the practical implementation of rights in the field of confidentiality, it is required to create a special state institution, the activity of which will be to ensure the safety of personal data and to protect person's private information. State activities should be aimed at ensuring information security and creating conditions for the safe exchange of information.

Thus, it is required to supplement the general system of legislation with legal relations in the field of the Internet. Particularly, it is required to establish administrative and criminal responsibility for the sale of personal data on the Internet, as well as for the distribution and transfer of personal photo and video materials without the person's consent.

REFERENCES

[1] Ugolovnyj kodeks Rossijskoj Federacii: [prinyat Gos. Dumoj 24 maya 1996 g.: odobren Sovetom Federacii 05 iyunya 1996 g.] // Sobranie zakonodatel'stva RF. – 1996. – No. 25. – St. 2954.

[2] Raab M. Zashchita setej: nakonec-to v centre vnimaniya / M. Raab – M.: Prosvyashchenie, 1994. – 18s.

[3] Veksler D. Nakonec-to nadezhno obespechena zashchita dannyh v radiosetyah[Tekst]/ D. Veksler – M.:Znaniya, 1996. – 13-14s.

[4]. Suhova S.V. Sistema bezopasnosti NetWare / S.V.Suhova –M.: Seti, 1995.- 60-70s.

[5] Belyaev V. Bezopasnost' v raspredelitel'nyh sistemah / V. Belyaev – M.: Mysl', 1997. – 36-40s.

[6] Vedeev D. Zashchita dannyh v komp'yuternyh setyah]/ D.Vedeev – M.:Prosvyashchenie, 1995. – 12-18s.

[7] Otchety po deyatel'nosti Analiticheskogo centra kompanii InfoWatch, [Elektronnyj resurs]. – URL: www.infowatch.ru/analytics/report

[8]. Lopashenko, N.A. Prestupleniya protiv sobstvennosti / N.A. Lopashenko. - M.: LeksEst, 2005. - 408 c.

[9] Gurskij, YU. Photoshop CS2 i cifrovoe foto. Luchshie tryuki i effekty / YU. Gurskij, M. Bondarenko, S. Bondarenko. - M.: SPb: Piter, 2007. - 208 c.

[10] Analogovaya i analogovo-cifrovaya vychislitel'naya tekhnika. - M.: NIIEIR, 1988. -647c.