Advances in Economics, Business and Management Research, volume 138
2nd International Scientific and Practical Conference "Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth" (MTDE 2020)

Digital Crime Concept

Rakhmanova E.N.[1], Pinkevich T.V.[2]

[1]*North-West branch of the Russian State University of Justice, Saint Petersburg, Russia*
[2]*Management Academy of the Ministry of the Interior of Russia, Moscow, Russia*

ABSTRACT
The 21st century is called the digital century. The digital world and modern mobile digital technologies are everywhere today. This shift in technology development brings not only huge benefits but also huge risks. Digital crime is one of the fastest-growing criminal activities, with more than a million people becoming victims of it worldwide every day. The peculiarity of these crimes is that, due to the development of digital technologies, the content of crime has changed; and most of it is committed in a virtual environment. For many years, the international community and states have been attempting to counter the commission of crimes using computer technology. Conventions, agreements, recommendations, and laws are adopted. But at present, they do not fully reflect the situation in this area. No less attention is paid to the problems caused by using modern technologies in the scientific literature. But there is no unity of opinion, most of the writings use such mostly outdated terms as "computer crime," "cybercrime", etc. At the same time, an analysis of the state of crime in this field, as well as of legislation and scientific literature, shows that there is a need for clarification of the existing concept of computer crime, expanding it to the concept of the "digital crime."
Keywords: *computer crime, digital crime, digital world*

1. INTRODUCTION

"In the 17th (seventeenth!) century, one of the geniuses of science, Professor Gottfried Wilhelm Leibniz, wrote that the future is inevitably connected with counting machines, which will be so perfect, objective, and efficient that they will impartially weigh the pros and cons and thus contribute, for example, to legal proceedings" [3, 122]. G. Leibniz's predictions come true; we see that the digital world is becoming an increasingly prominent part of our daily lives, which is associated with digital technology, digital economy, digital security, and, finally, with digital crime [8]. The digital world and its potential extend to all spheres of activity of modern society, rapidly displacing the old way of life, old thinking, and legacy technologies.
The development and rapid widespread dissemination of digital technology contain a serious potential for criminological risks, which in modern society "is the background that unfolds and the factor that determines the main fields of the country's criminal policy. The area of these risks is our entire reality, without exception, all areas of manifestation of human activity, which either consciously generates,

or allows the possibility of some dangerous and harmful consequences" [2]. There is no coincidence that this topic became the subject of discussion of the Conference of the Council of Europe "Justice in Europe in the Face of Digital Challenges," which was held on October 15, 2019, in Strasbourg.
In this regard, the so-called digital crime, the counteraction of which today is impossible to recognize as sufficient, is of special concern. According to experts, the annual losses from it range from 55 million to 13 billion US dollars per year [9, 10]. At the same time, it is practically impossible to assess the true scale of the social consequences of digital crime since not all victims are always aware that they are victims of such crimes, just as it is impossible to determine the real number of victims in the case of phishing and hacker attacks, etc.
The existing legal framework for combating digital crime and other components of anti-criminal tools are still under development. An important factor complicating the definition of digital crime is the so-called jurisdictional dilemma since this term in different countries is understood and defined differently. Moreover, there are no appropriate specific statistics on the committed crimes of this type. The same problem is present in Russia as well, where the concept of "digital crime" is currently absent at the legislative level.

2. STUDY METHODOLOGY

In the course of the study, systemic, synergetic, and simulation approaches were used, which is due to the nature of digital crime and related phenomena [1], as well as general scientific (systemic, structurally functional, statistical, prognostic, etc.), and special methods (formal-logical analysis, comparative-legal research, etc.).

3. RESEARCH RESULTS

Computer crimes and the need to define them have been discussed for over 40 years. It is known that the term "computer crime" was first used in one of the reports of the Stanford Research Institute. Later in the paper on cybercrime, the following classification was adopted: computer as a subject of crime; computer as an object of crime; or a computer as a tool (the fourth option, proposed in 1973, computer as a symbol, was apparently removed from the use in the 1980s).

For the first time, the problems of preventing computer crimes were considered at the Eighth Congress on the Prevention of Crime and the Treatment of Offenders, held in 1990. The UN is actively reviewing various aspects related to the use of computers. In 1992, the OECD drafted "Directives on the Security of Information Systems." They were subsequently revised and adopted on July 25, 2002, as Recommendations of the OECD Council, "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security."

Cybercrime was defined in 2000 at the Tenth UN Congress on Crime Prevention and Criminal Justice. It was recognized that computer crime relates to any criminal act, "which may be committed using a computer system or network, within a computer system or network, or against a computer system or network. In principle, it covers any crime that may be committed in an electronic environment."

But as early as at the Eleventh United Nations Congress on Crime Prevention and Criminal Justice (2005), it was proposed to "formulate this conceptual model in another way, considering computer-related crimes as behavior prohibited by law and/or judicial practice, which a) is directed actually in the computer field and communication technology; b) includes the use of digital technology in the commission of an offense; or c) includes the use of a computer as a tool in the process of committing other crimes, and, accordingly, the computer serves as a source of electronic procedural evidence."

The Fourteenth UN Congress on Crime Prevention and Criminal Justice is about to take place in Kyoto on April 20-27, 2020. At the Workshop "Modern Trends in Crime, Recent Changes, and New Solutions, Particularly, the Use of Modern Technology as a Means of Committing a Crime and a Tool to Combat Crime," it is again planned to discuss the problems of using modern technology in committing crimes. Moreover, it should be noted that in the preliminary materials of the Congress, the concepts of "cybercrime" and "computer" are practically not used. It is about modern information and digital technologies.

The Council of Europe Convention (Budapest) classifies this type of crime as computer crime and subdivides it into three groups: "crimes against the confidentiality, integrity, and availability of computer data or systems," "offenses related to the use of computer tools," and "offenses related to the content of computer data."

In the post-Soviet space, the definition of computer crime is given in the Agreement on Cooperation between the CIS Member States in the fight against Computer Information Crimes, which defines "computer information crime." It was recognized that it constitutes "a criminal offense, the subject of which is computer information." Computer information includes information stored in computer memory, on a computer or other media in a form compatible with the computer or transmitted through communication channels. But in 2018, a new document was prepared in Dushanbe (it has not yet come into force), which is dedicated to the struggle of the CIS countries with crimes in the field of information technology; actually, the point is still in crimes in the field of computer information.

The Model Criminal Code of the CIS states also establishes liability for computer crimes.

Thus, the concept of "digital crime" is practically absent in international acts, most international acts use the term "computer crime," which is understood as any action, in which computers, computer networks, as well as digital technologies, are the tool, the target, or the place of criminal actions.

The legislation of foreign countries uses not only the terms "computer crimes" but also the terms "electronic communications," "information technology," or "crime in the field of high technology."

Moreover, while initially the legislation of most countries was focused on the protection of tangible objects and confidentiality, then laws on criminal responsibility for other crimes began to be adopted later. For example, personal data protection laws have been passed in Sweden, the USA, Germany, Austria, Denmark, France, Norway, Luxembourg, Iceland, Israel, Australia, Canada, the UK, Finland, and so on. Since 1978, laws to combat economic computer crimes have been passed in the USA (in state law) and in Italy, Australia, the UK, Canada, Denmark, Germany, Sweden, Austria, Japan, Norway, and other countries. Recent decades, Austria, Bulgaria, the UK, Hungary, Finland, Italy, Lithuania, Slovakia, Slovenia, etc. are characterized by the adoption of laws aimed at protecting against cyber violence in its various forms.

In 2009, a new era began, the era of cryptocurrency. Currently, there is no unified global approach to this phenomenon. A number of countries, such as the USA, Canada, Australia, Finland, etc., have adopted legislative acts regulating such activities and recognizing their legitimacy. While some countries are cautious due to the instability of cyber currency, a decentralized nature, the perceived threat to existing currency systems, and links to illegal activities, such as drug trafficking and money laundering. As a result, some countries have completely banned digital currency, while others are trying to ban any support from the banking and financial system required for its trade and use (China, Russia, Vietnam, etc.).

The Russian Federation also does not ignore the new challenges arising from the rapidly developing digital technologies.

Within the framework of criminal legislation, Chapter 28 of the Criminal Code of the Russian Federation is specifically devoted to crimes in the field of computer information, which provides for responsibility for unauthorized access (Article 272), creation, use, and

distribution of malicious computer programs (Article 273), violation of the rules for operating storage facilities, processing, or transmission of protected computer information or information and telecommunication networks and terminal equipment, as well as access rules to information and telecommunication networks (Article 274), and finally, undue influence on the critical information structure of the Russian Federation (Art. 2741).

The use of information and telecommunication networks (including the Internet) for criminal purposes is provided for in the 17 provisions of the Special Part of the Criminal Code of the Russian Federation. Since the beginning of 2017, actions committed using computer and telecommunication technologies began to stand out as a separate line in criminal statistics when accounting crimes of an economic nature.

Therefore, all crimes in the criminal legislation of Russia may be conditionally divided into those that are purely computer-based (Chapter 28 of the Criminal Code of the Russian Federation, if we talk about Russian criminal legislation) and those that are committed through the use of information and telecommunication networks, whereupon modern information technology is not the purpose of these crimes.

Analysis of the literature on crimes committed using modern technology shows that it does not provide a complete picture and definition of those crimes that are committed in the field of digital technology or using digital technology [10]. Terms such as "electronic crime," "computer crime," "crime committed using computer technology," "high-technology crime," "cybercrime", etc. [4] are used.

Most often, it is alleged that the computer is the purpose of the crime [11, 207] or the point is in traditional crimes but committed using computer technology [6, 3]. This can be fraud, theft, various types of violent crimes, the dissemination of personal information, slander, etc. [5].

A number of dissertation and scientific studies in the Russian Federation are also devoted to this problem but they are mainly about crimes committed using information and telecommunication networks and the Internet, to which the authors attribute crimes in the field of computer information.

4. DISCUSSING THE RESULTS

At present, we have to admit that modern digital technologies are a key component of most, if not all, crimes committed. "Thus, according to cybersecurity organizations, by 2021, the damage from cybercrime could reach $6 trillion compared with 3 trillion in 2015, which will exceed the profits from the global trade in narcotic drugs of all kinds. This information is confirmed by leading experts and international companies in the field of cybersecurity (Oracle, McAfee), which proceed in their forecasts from the analysis of statistical crime indicators of past years, as well as rely on studies in the field of organizing cyber attacks also tending to increase significantly by 2021" [11, 557].

The concept of digital crime is usually replaced by such terms as cybercrime, electronic crime, computer crime, etc. Despite the fact that, unlike traditional crimes, digital crime has its own unique features. It has no geographical boundaries; digital crime can be committed in one country or region against other countries or regions. Despite the fact that the digital world gives rise to a sense of anonymity and impunity when committing a crime using digital technologies, criminals leave a digital trace [8, 13]. The place where the digital crime is committed is the virtual environment; computer data, digital systems, or social media are used to commit it.

It should be recognized that the Internet today has acquired new quality and content. In many respects, this was facilitated by the development of the digital space, which covers not only computer technologies but also network ones, Internet resources, electronic computers, etc. In the last decade, the number of crimes involving cell phones has been growing inexorably, a new type of criminal activity associated with the so-called cloud technologies has emerged [7]. Experts predict the further development of artificial intelligence, blockchain, big data, digital twins, cloud programs, and chatbots integrated into various platforms, which will also change the way people interact with the digital world. Digital life will continue to further expand the boundaries and opportunities of people. Digital life is gradually going beyond the scope of the computer; more and more new products are emerging.

All this allows saying that the concept of the "digital crime" is broader than the concept of the "cybercrime" or computer crime. Digital crime includes a wider range of illegal actions, including those committed both in the field of and with the use of digital technologies, including in a virtual environment that complements our reality [8].

5. CONCLUSION

Today, digital technology is used everywhere. Widely used are computers, laptops, tablets, smartphones, mobile phones, and so on. The main goal of digital technology is to establish a connection between people quickly, effortlessly, and with minimal cost. People are connected to each other by a huge range of digital services and resources. Digital information is very different from its physical counterpart, it can be quickly duplicated, distributed in a controlled manner, and stored in different places.

However, digital capabilities make crime easier. A feature of these crimes is that today they are not limited by state borders, they can be committed from anywhere and against any user located anywhere in the world. There is no doubt that digital crime is not like an ordinary crime, it has its own distinguished features, with no exception to computer crime. For example, digital evidence of a crime can be easily changed or damaged.

Today, digital crime requires serious efforts from states to combat it. The effectiveness of countering it, first of all,

depends on an international agreement on a unified approach to the definition of this phenomenon.
Digital crime is a social unlawful phenomenon, which includes a set of crimes committed in the field of or with the use of digital technologies, including the illegal acquisition and offering or dissemination of information in information and telecommunication networks, as well as in a virtual environment that complements reality.

REFERENCES

[1] S.E. Vitsin, Systematic approach and crime, Moscow: Acad. control Ministry of Internal Affairs of Russia, 1980.

[2] M.M Babaev. Risks as a component of the determination complex of crime, Bulletin of the Nizhny Novgorod Acad. of the Ministry of Internal Affairs of Russia, 1(41) (2018) 104-110

[3] V.E. Kvashis, On the new theory of applied criminology: review of the textbook V.S. Ovchinsky “Criminology of the digital world”, Society and Law, 1(63) (2018) 122-124

[4] Y. Chang, Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention Across the Taiwan Strait. Cheltenham UK: Edward Elgar Publishing, 2012.

[5] Crime in the age of technology. Available at: URL: https://www.cepol.europa.eu/sites/default/files/924156-v7-Crime_in_the_age_of_technology_.pdf

[6] M. D. Goodman, S. Brenner,The Emerging Consensus on Criminal Conduct in Cyberspace, Int. J.Law and Inf.Tech., 10 (2) (2002) 139-223

[7] Bert-Jaap Koops, M.Goodwin, Cyberspace, the Cloud, and Cross-Border Criminal Investigation. The Limits and Possibilities of International Law (December 20, 2014). Tilburg Institute for Law, Technology, and Society CTLD – Center for Transboundary Legal Development, December 2014; Tilburg Law School Research Paper No. 5/2016. Available at SSRN: https://ssrn.com/abstract=2698263 or http://dx.doi.org/10.2139/ssrn.2698263

[8] S. Mohammed, An Introduction to Digital Crimes, Int. J. in Found.of Comp. Sci. & Tech. (IJFCST), vol 15-3 (2015) 13-24

[9] D. B. Parker, Fighting Computer Crime: a new framework for protecting information, John Wiley & Sons, NY United States, 1998.

[10] G. Stratton, A. Powell, R.Cameron, Crime and Justice in Digital Society: Towards a "Digital Criminology"? Int. J. for Crime, Justice and Soc. Democracy 6 (2) (2017) 17-33. DOI: 10.5204/ijcjsd. v6i2.355

[11] A.P. Sukhodolov, E.A. Antonyan, M.V. Rukinov, M.Yu .Shamrin, M.G. Spasennikova, Blockchain in digital criminology: problem statement. Vserossiiskii kriminologicheskii zhurnal, Russian J. of Criminology, vol. 13-4 (2019) 555–563. DOI: 10.17150/2500-4255.2019.13(4).555-563.

[12] R. A. Spinello, Regulating Cyberspace: The Policies and Technologies of Control. Greenwood Publishing Group. United States, 2002.