REICE
Revista Electrónica de Investigación en Ciencias Económicas
Abriendo Camino al Conocimiento
Facultad de Ciencias Económicas, UNAN-Managua

Vol. 10, No. 19, Enero - Junio 2022 REICE ISSN: 2308-782X

http://revistacienciaseconomicas.unan.edu.ni/index.php/REICE
revistacienciaseconomicas@gmail.com

Crime Prevention in The Digital Economy
Prevención del delito en la economía digital

Fecha recepción: enero 01 del 2022
Fecha aceptación: enero 19 del 2022

Dmitriy A. Ivanov
Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs of the Russian Federation (MGIMO-University), Moscow, Russia.
Email: dmitriy.a.ivanov@bk.ru
ORCID: https://orcid.org/0000-0002-2023-3771
Anastasiia M. Sachek
Moscow State Institute of International Relations (University) of the Ministry of Foreign Affairs of the Russian Federation (MGIMO-University), Moscow, Russia.
Email: sachek.a.m@mail.ru
ORCID: https://orcid.org/0000-0001-7686-4954
Elena N. Kleshchina
Kutafin Moscow State Law University (MSAL), Moscow, Russia.
Email: kleshchina.e.n@mail.ru
ORCID: https://orcid.org/0000-0001-8838-4544
Anna V. Skachko
Krasnodar University of the Ministry of internal Affairs of Russia, Krasnodar, Russia.
Email: skachko.a.v@yandex.ru
ORCID: https://orcid.org/0000-0002-2878-8413
Elena V. Blinova
Plekhanov Russian University of Economics, Moscow, Russia.
Email: e.v_blinova@mail.ru
ORCID: https://orcid.org/0000-0003-2554-0372
Svetlana I. Antimonova
Moscow University of the Ministry of Internal Affairs of Russia named by V.Ya. Kikot, Moscow, Russia.
Email: svetlana.i.antimonova@mail.ru
ORCID: https://orcid.org/0000-0001-7169-7915

Resumen

En el presente artículo, los autores abordan el proceso de digitalización de la economía y el aumento de la delincuencia en la economía digital. Consideran las razones de la latencia del delito cibernético, los problemas de definición de los delitos cometidos en la esfera de las tecnologías de la información y su clasificación. Los autores proponen medidas específicas destinadas a prevenir la delincuencia en la economía digital. La más importante de estas medidas es el desarrollo de sistemas nacionales innovadores, que se espera que garantice el crecimiento económico y aumente la competitividad de la economía digital nacional.

Palabras clave: Economía Digital; Digitalización; La seguridad cibernética; Ciberdelito; Contrarrestar el crimen; Detección e investigación de delitos.

Abstract

In the present article, the authors address the process of digitalization of the economy and the increased crime in the digital economy. They consider the reasons for the latency of cybercrime, the issues of defining criminal offences committed in the IT sphere, and their classification. The authors propose specific measures aimed at preventing crime in the digital economy. The most important of these measures is the development of national innovative systems, which is expected to ensure economic growth and increase the competitiveness of the national digital economy.

Keywords: Digital Economy; Digitalization; Cyber-Security; Cybercrime; Counteracting Crime; Crime Detection And Investigation.

.

Introduction

Nowadays, the life of society is becoming more and more defined by the widespread use of computer technologies and the increase in the volume of digital data flows. Non-standard pricing models related to involving the users in the creation of the value chain are emerging, since the provision of digital services largely depends on user data. As a result, the perception of economic activity is changing.

Materials and Methods

While writing the present article, the authors mainly used the general scientific systematic method of cognition, which made it possible to comprehensively consider and fully analyze controversial issues related to crime prevention in the digital economy of the Russian Federation. The systematic approach made it possible to consider organizational and procedural aspects of crime prevention in the digital economy. The comparative legal analysis allowed the authors to examine in detail the domestic legislation system that regulates the activities of state bodies and officials regarding the prevention of crime in the digital economy. Using this method, the authors were able to identify existing problems and propose possible solutions to them, as well as specific measures aimed at preventing crimes emerging in the new era. The application of analysis and synthesis methods made it possible to identify existing problems in the law enforcement practice of preventing cybercrimes against the economy. As a result of applying the above-mentioned methodology, the authors acquired knowledge which can help to improve activities related to crime prevention. That includes a better understanding of trends in legislative improvement aimed at increasing the efficiency of state bodies and officials who are entrusted with the responsibility to disclose and investigate crimes, as well as contribute to their prevention.

Result and discussion

Today, conventional economic activities are undergoing digitalization: trade in goods and banking services are being brought to the digital space. At the same time, fundamentally new types of economic activity appear, including the creation of targeted advertising based on user data, the provision of access to digital data (music, video) for a subscription fee, and crowdfunding.

That said, new ways of doing business based on the use of digital technologies are emerging. These are known as digital “business models” that consist in providing digital services. According to the definition given by the European Commission, a digital service is “a service that is delivered over the Internet or an electronic network, and the nature of which renders its supply essentially automated and involving minimal human intervention” on the side of the supplier (Proposal for a Council Directive laying down rules relating to the corporate taxation of a significant digital presence, 2018, p. 7).

The digitalization of the economy is continuing to gather momentum. In 2006, among the 20 largest companies in the world by market capitalization, there was only one technology company (with a market capitalization share of 7%). After a little more than a decade, in 2020, digital companies occupied 6 positions out of 20. The total share of their market capitalization amounted to 54% (Communication from the Commission…, 2017, p. 4).

Despite all the benefits associated with the digitalization, there is also a negative side to it: the modernization of crime (Sukhodolov et al., 2017, p. 259). It is undeniable that progress affects all spheres of public life, including the tools for committing crimes (Sazonova, 2021). Information and communication technologies have become convenient means and instruments for committing many kinds of crime (Pushkarev et al., 2020a, p. 244-248). Due to this factor, crimes committed in the digital economy are stand-alone among economic crimes in general (Pushkarev et al., 2019, p. 2563 2566). It is not by chance that in record-keeping covering the registration of all criminal offences, those committed “using information and telecommunication technologies” (ITC) or “in the field

of computer information" constitute a separate group. Among them, one can note digitalized economic crimes, for example, fraud (articles 159, 159.3, 159.6 of the Criminal Code of the Russian Federation).

However, of course, crimes committed in the IT sphere are not limited to economic crimes. Again, crimes committed in the IT sphere include all computer facilitated crimes committed "using information and telecommunication technologies" or "in the field of computer information". Despite the fact that the statistics published by the Ministry of Internal Affairs of Russia reflect a large number of such crimes (including those qualifying under articles 205.2, 228.1, 242, 242.1, 242.2, 280 of the CC), some experts believe that the Ministry has adopted a rather narrow approach to their qualification (Sazonova, 2021). These experts justify their claims by the fact that ICT prevails in most aspects of society, and, accordingly, the concept of "crimes committed in the IT sphere" can cover most of the criminal offences specified in the Criminal Code.

To outline the range of these crimes to the full extent, one can refer to the Budapest Convention on Cybercrime No. 185 (23rd of November 2001), keeping in mind, however, that Russia has not adhered to it. Based on the provisions of this Convention, cybercrimes include:

1. Offences specified in Chapter 28 of the Criminal Code of the Russian Federation, the group object of which resides in social relationships in the sphere of computer information (art. 272, 273, 274, 274.1);
2. Crimes whose target is digital information and its carriers. For example, violation of copyright and neighboring rights (art. 146); crimes related to the illegal receipt and disclosure of confidential information (art. 183); illegal circulation of means of payments (art. 187); illegal production and distribution of pornographic materials or objects (art. 242);
3. Crimes whose objective aspect includes actions related to misrepresentation of digital information. For example, falsifying the Comprehensive State Register of Legal Entities (art. 170.1);
4. Crimes whose objective aspect consists in actions related to transfer and distribution of digital information. For example, libel (art. 128.1); public calls for committing terrorist

activities, public justification of terrorism or its propaganda (art. 205.2), public appeals for the performance of extremist activity (art. 280);

5. Crimes whose modus operandi may involve or necessarily does involve the use of information technologies. The use of information and telecommunication technologies can be directly indicated as a feature of a certain crime: both constitutive (part 1 of article 183 of the Criminal Code - "as well as in other illegal ways"), and qualifying (part 2 of article 205.2 - "committed through the use of electronic or information and telecommunication networks, including the Internet"). However, sometimes the legislator resorts to a less casuistic way of constructing the disposition of the legal rule by not excluding the possibility of using ICT, though not stating it explicitly (art. 185.6) (Sukhodolov et al., 2017, p. 260).

Thereby, one cannot rule out the possibility that the data published by the Ministry of Internal Affairs of Russia does not reflect the full scale of criminal risks associated with the illegal use of information and communication technologies. However, the statistics provided by the Ministry are sufficient to conclude that there has been a significant increase in cybercrime. From January to March 2020, the number of crimes committed in the IT sector represented an 83.9% increase over the number in the same period in 2019. It is the factor with which the Ministry associates the 4% increase in the crime rate in general.

In the first three months of the year 2021, there was an increase in the number of felonies (grave and especially grave crimes, in the terms of the Russian criminal law), which was as well related to the increase in the number of crimes committed using ICT (33.7% more crimes were committed in the IT sector than in the same period in 2020). Notably, the number of crimes committed with the use of the Internet and mobile communications increased by 51.6% and 31.6% respectively.

During the period from January to March 2021, the law enforcement bodies detected 135,780 crimes committed “using information and telecommunication technologies” or “in the field of computer information” (crimes against property constituted the majority of

those: fraud – 43%, theft – 31%). The share of such criminal offences in the overall number of registered crimes stood at 27.1%.

It seems reasonable to assume that such discouraging figures can be explained by the necessitated transition to telecommuting. As the OECD notes, today's reliance on digital solutions has created a fertile environment for cybercriminals (OECD Digital Economy Outlook 2020, 2020). However, given the latency of cybercrime and the fact that these figures only reflect the number of registered crimes, it is important to not mistake these numbers for the true extent of cybercrime. Latency of cybercrime is linked to the following factors:

- continuous change in technical methods of recording, processing and storing information and the resulting difficulty of designating the range of cybercrimes;
- constant transformation of the means for committing crimes as well as the objects of the offences in question.

Another reason for the difficulty of cybercrime detection is the fact that cybercrimes often form aggregations with other offences and cannot always be qualified correctly. This conclusion was drawn by A.P. Sukhodolov, L.A. Kolpakova and B.A. Spasennikov, who have studied 150 convictions. Crimes committed in the digital economy served as the object of their research. They noted that most often the charges included, along with the crimes in question, offences specified in articles 272-274 of the Criminal Code of the Russian Federation (crimes in the sphere of computer information) (Sukhodolov et al., 2017, p. 260).

In addition, as noted by some scientists (Sukhodolov et al., 2017, p. 261), the State's legislative response to cybercrime is at times inefficient due to the rapid development of technical means for committing crimes. For example, article 273 of the Criminal Code establishes criminal liability for the creation, use and dissemination of malicious computer programs, but does not criminalize the use of other technical means aimed at violating digital security systems, such as software for decrypting information and password sniffing or port scanners for hacking networks.

One can argue that crimes committed in the digital economy form a separate group of cybercrimes. Just as there is no unanimity of views on the classification of all the crimes committed in the IT sphere, experts express different opinions as to which offences specified in the Special Part of the Criminal Code can be included into this specific group of cybercrimes.

Since economic crimes are specified in Section VIII of the Criminal Code, it is reasonable to assume that offences committed in the field of the digital economy can be found among those provided for in Chapter 21 (crimes against property) and Chapter 22 (crimes in the sphere of economic activity). In the course of a survey carried out by A.P. Sukhodolov, L.A. Kolpakova and B.A. Spasennikov, 89.8% of experts argued that crimes in the digital economy include those the constitutive feature of which is the use of information and telecommunication technologies, as well as electronic means of payment (i.e. crimes provided for in articles 159.3, 159.6, 171.2, 185.3, 187 of the Criminal Code). Less often, the respondents mentioned corpus delicti of articles 159, 172.1, 172.2, 174, 180, 183, 185.6 (Sukhodolov et al., 2017, p. 263).

The existing rules of electronic environment operation make possible the anonymity of actions done in the network, which significantly complicates the identification of criminals and prevents the development of measures aimed at preventing such crimes. Crime prevention, alongside with fighting crime and controlling its level, is a form of counteracting crime. To prevent crimes committed in the digital economy, state bodies must undertake activities that have an impact on the causes and conditions conducive to the commission of crimes, as well as on those who commit them (Gavrilin et al., 2019, p. 167). Such activities are carried out at three levels, each characterized by the application of specific measures:

1. General social level;
2. Special criminological level;
3. Individual (victimological) level.

The measures taken at the so-called general social level aim primarily at solving a set of social adversities that engender, among other things, the rise in crime committed in the digital economy sphere. The application of measures at this level of crime prevention does not have a direct purpose of making an impact on criminogenic processes. Nevertheless, solving social problems can help to eliminate the conditions (and, in some cases, the reasons) for the commission of specific types of crimes.

At the general social level, economic, social, scientific, technical and legislative measures are taken. The economic measures taken at the social level include the development of national innovative systems, which can ensure economic growth by increasing the competitiveness of the national digital economy. Social measures consist in counteracting social and property stratification. Scientific and technical measures include state support for research aimed at strengthening national information security by limiting the possibilities to illegitimately gain access to digital information and by creating conditions for the functioning of information and communication technologies. Legislative measures include, first and foremost, the elimination of legal gaps that impede the activities of law enforcement bodies in their fight against crime. For example, there has been a proposal to legislate the obligation of computer manufacturers to install anti-virus protection systems in their products. The legislative measures also include the conclusion of international treaties aimed at counteracting crime in the IT sector, in general, and in the digital economy, in particular. Adherence to international treaties is necessary because the Internet obviously does not have any borders, and, thereby, cybercrime is moving to a transnational organized level (Gavrilin et al., 2019, p. 60).

In contrast to the measures undertaken at the general social level of crime prevention, measures of the special criminological level are aimed directly at eliminating the causes and conditions for committing crimes in the digital economy. Firstly, these measures include the scientific support of crime prevention activities, i.e. the use of the results of research in law enforcement practice. Secondly, they provide the methodological support of crime prevention activities that consist in refining subordinate legislation that contributes to a prompt response to crimes committed in the digital economy as well as an effective

application of legislative acts. Thirdly, some of these measures are organizational ones, consisting in the training of law enforcement officers and in the transition from the territorial principle of their work to a functional one. Since cybercrime, in general, and crime in the digital economy, in particular, is cross-border in nature, it is almost impossible to determine the exact place where the crime was committed and, thereby, to entrust its investigation to a specific territorial authority (Pushkarev et al., 2020b, p. 333-334).

The individual (or victimological) level of crime prevention is also of great importance, since the behavior of the victim is one of the elements of the crime mechanism. Measures taken at the individual level consist in educating the population about the rules of safe conduct in cyberspace, as well as informing the organizations of various forms of ownership about the importance of ensuring the security of their information systems.

Conclusion

Thus, a negative consequence of the digitalization of the economy is the modernization of the means and instruments for committing crimes, which, in turn, contributes to the high latency of cybercrime. Crimes committed in the digital economy are stand-alone among economic crimes and the activities undertaken by the state bodies to prevent such crimes should be of a multi-level character and consider the issues of qualifying such criminal offences.

Referencias Bibliográficas

1. Communication from the Commission to the European Parliament and the Council, A Fair and Efficient Tax System in the European Union for the Digital Single Market. (2017). Official Journal of the European Union, COM/2017/547 final.

Retrieved from: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017DC0547

2. ETS Convention on Computer Crime No. 185 (Budapest, 23 November 2001). Council of Europe. Retrieved from: https://base.garant.ru/4089723/
3. Gavrilin, Yu.V., Anosov, A.V., Baranov, V.V. (2019). Activities undertaken by the internal affairs bodies to fight crimes committed with the use of information, telecommunication and high technologies: manual: in 2 parts. Moscow: Academy of Management of the Ministry of Internal Affairs of Russia.
4. OECD Digital Economy Outlook 2020. (2020). Organization for Economic Cooperation and Development: official website. Retrieved from: https://www.oecd.org/digital/oecd-digital-economy-outlook-2020-bb167041-en.htm
5. Proposal for a Council Directive laying down rules relating to the corporate taxation of a significant digital presence. (2018). Official Journal of the European Union, COM/2018/0147 final. Retrieved from: https://ec.europa.eu/taxation_customs/sites/taxation/files/proposal_significant_digital_en.pdf
6. Pushkarev, V.V., Artemova, V.V., Ermakov, S.V, Alimamedov, E.N., Popenkov, A.V. (2020b). Criminal prosecution of persons, who committed criminal, acts using the cryptocurrency in the Russian Federation. Revista San Gregorio, 42, 330-335.
7. Pushkarev, V.V., Boziev, T.O., Esina, A.S., Zhamkova, O.E., Chasovnikova, O.G. (2020a). Criminal prosecution for crimes committed in the banking industry. Laplage em Revista (Sorocaba), 6(ExtraC), 244-248.
8. Pushkarev, V.V., Gaevoy, A., Skachko, A.V., Kolchurin, A., Lozovsky, D.N. (2019). Criminal Prosecution and Qualification of Cybercrime in the Digital Economy. Journal of Advanced Research in Dynamical and Control Systems, 11(8), 2563 2566.
9. Sazonova, M. (2021). Criminal and legal risks in the context of digitalization: methods of counteraction. GARANT.RU. Retrieved from: https://www.garant.ru/news/1443692/#sdfootnote1sym

10. Sukhodolov, A.P., Kolpakova, L.A., Spasennikov, B.A. (2017). Issues of countering crimes in the sphere of digital economy. All-Russian criminological journal, 2, 258-267..