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)

Major Aspects of Criminal Law Protection in Digital Economy

Reshnyak M. G.[1,*] Borisov S.V.[2]

[1]*Moscow state University of international relations (MGIMO, MFA of Russia) Odintsovo branch, International law faculty, Department of criminal law, criminal procedure and criminalistics, Chair Assistant Professor, PhD in Law, associate Professor*
[2]*Institute of Legislation and Comparative Law under the Government of the Russian Federation, Moscow, Russia*
[*]*Corresponding author. Email: irbis-7375@yandex.ru*

ABSTRACT
Recent years are characterized by further development of the information society as a whole and digital economy as its integral part, based on the widespread use of information and communication technologies in various fields of economic activity. Both positive effect of such technologies rapid development including their spread in economic relations and the enhanced use of new ways of committing crimes against property and other social relations in the field of economy can be observed. Such ways are mainly limited to a guilty persons' use of the Internet and other data telecommunication networks vast opportunities. These circumstances require legislator's prompt response aimed at forming scientifically based measures to ensure appropriate digital economy protection in modern conditions. The article distinguishes and considers different modern problems of criminal law protection of social relations concerning formation and functioning of digital economy in the Russian Federation. The authors analyze the current criminal legislation in terms of ensuring markets and industries effective functioning in the digital economy field. Based on the study, proposals for further development of criminal measures for the crime prevention are formulated.
Keywords: *economic crimes, state criminal policy, criminal protection of social relations, information and communication technologies, digital economy*

1. INTRODUCTION

It is impossible to imagine modern society and the existing economic relations without the extensive use of various digital technologies including the Internet and other data telecommunications networks. Nowadays, digitalization affects almost all spheres of society and serves as a 'driver' of development in economic and other fields. In this connection, the emergence and development of the information society and digital economy as its integral part, can be noted [9, 2-3; 10, 5-7].

The society is characterized by such amounts of information and the level of its application and accessibility that it affects citizens' economic and socio-cultural living conditions dramatically as follows from Section 4 of the Strategy for the Development of the Information Society for 2017-2030 (hereinafter referred to as the Strategy for the Development of the Information Society). Digital economy defined as economic activity is one of the main elements of the information society. Compared with the indicators of traditional forms of economic activity, digital data is the key factor of production for processing large volumes of data and using the analysis results, which contribute to a significant increase in the efficiency of various types of production, technology, equipment, storage, sale and delivery of goods and services.

Vaypan V.A. considers digital economy as an established system of economic relations, where digital data that is actively used in operations in all economic areas is the distinctive feature and the leading factor. Digital economy involves a wide range of electronic and digital technologies, with the main focus not on software, but on goods, services and facilities that are provided through e-business (e-Commerce) [3, 13-14]. In other words, the more conclusive finding is that the use of digital data technologies that characterize this sector of economy is inherent not only to production, but also the exchange and distribution of its benefits.

If we compare a traditional market, which operates with conventional goods, and a digital economy, we can conclude that the latter is distinguished by the virtual economic ties and document circulation, a considerably lower requirement for raw materials supplies, an avoidance of redundant transportation infrastructure, an expedited traffic on a global scale, the use of modern digital currencies and etc.

Features and trends in the development of a digital economy require legal framework of relevant economic activity improvement and, moreover, law-making work should be comprehensive and systematic, cover all branches of law both regulatory and protective, including

criminal law rules that provide for liability for socially dangerous actions that can significantly disrupt social relations in the digital economy field. Taking into account that such rapid development of IT-technologies interconnects with the state security, this direction draws great attention coupled with potential risks associated with the development of IT-technologies and the expansion of their use for illegal purposes specified in the Information Society Development Strategy.

2. MATERIAL AND METHODS

At the same time, the study of current criminal legislation of the Russian Federation leads to the conclusion that it has not paid due attention to creating a system of measures tailored the specifics of encroachments on the digital economy so far. We believe that this area of improving the legal framework should be given importance as a constituent of the set of measures to ensure the steady development of the national digital economy, planned and undertaken by our state in recent years.

Doctrinal studies on the digital economy development affect mainly the problems of improving the norms of the arbitration procedure, civil, civil procedure, information, labor and other branches of the Russian legal system as well [1; 3; 4; 6], while the criminal-legal aspect of the corresponding area is mainly considered on a piecemeal basis, and, moreover, the main content of the relevant scientific works is usually devoted to the criminological characteristics and prevention of criminal offences in this field [2; 5; 7; 8].

In addressing section VIII of the Criminal Code of the Russian Federation (hereinafter referred to as "RF Criminal Code"), which systematizes the rules on liability for economic crimes, we paid attention to the fact that the use of information and communication technologies, which as a rule increases the level of public danger of the actions concerned, is gradually taken into account by the legislator as a constitutive or qualifying attribute of different similar encroachments. However, in our opinion, this direction of legislative activity has deficiencies associated with deviations from the requirements of consistency and legal certainty in the regulation of criminal law protection of social relations in the economic field. Given the limitations of this study, we will focus on the problems of regulating this attribute in the articles of Chapter 21 of the RF Criminal Code.

Thus, in 2012, Chapter 21 of the RF Criminal Code on Crimes Against Property was supplemented by new articles on various types of fraud, including article 1596 on criminal liability for fraud in computer information field.

Meanwhile the general notion of fraud contained in the disposition of Part 1 of Art. 159 of the RF Criminal Code includes such constitutive sign of committing fraud as an alternative way that distinguishes it from other forms of property embezzlement – deceit or abuse of trust that are associated with misleading another person. This fact is not taken into account in the legislative definition of fraud in computer information field. The analysis of the definition of fraud in computer information field (part 1 of article 159 of the RF Criminal Code) allows us to conclude that it is an independent form of theft or property of another right acquisition, which differs by its specific way of committing a crime that produces effects on computer information (input, deleting, blocking and modification) or on its data storage, processing or transfer, as well as on data telecommunication networks (interference in the operation). In this case, that means that there is no effect on man, and therefore there is no fraud, so the use of this concept to denote another crime is a true deviation from the stated requirements of legal certainty and consistency.

3. RESULTS AND DISCUSSION

This problem exacerbated when in 2018 part 3 of Article 158 of the RF Criminal Code on legal liability for theft was supplemented by a new special qualifying attribute which imposes a heavier punishment for covert embezzlement by debiting from a bank account or by means of electronic money if there are no indicators of electronic payment instrument fraud (article 1593 of the RF Criminal Code). In this regard, it should be noted that originally Article 1593 of the RF Criminal Code contained a special fraud type definition based on the attributes specified in the general rule (Article 159 of the RF Criminal Code), implying the embezzlement by using a fake or other person's credit card and deceiving a credit, trade or other organization's authorized employee. After the amendments made to Article 1593 of the RF Criminal Code together with the above-mentioned addition to part 3 of Article 158 of the RF Criminal Code legislative regulation of liability has lost its legal certainty for this type of fraud. At present, there is no reference to modus operandi and the fact that fraud concerns just another person in the disposition of part 1 of Article 1593 of the RF Criminal Code. However, none of this exclude a reference to the general concept of fraud set forth in part 1 of article 159 of the RF Criminal Code, where such method is proposed.

In addition, electronic payment instrument that is defined in paragraph 19 of Art. 3 of the Federal Law "On the National Payment System" as an instrument and (or) method allowing the client of the operator to make, certify and transfer orders for the purpose of money transfer in non-cash forms with the help of information media technologies and digital cash including bank cards or other technical means, was declared instead of bank cards and other people's property in part 1 of Article 1593 of the RF Criminal Code. Thus, not only the legal certainty of this criminal prohibition was lost, but also essential competition arose between the latter and the provisions of clause "g" of part 3 of Article 158 of the RF Criminal Code and Art. 1596 of the RF Criminal Code.

4. CONCLUSION

Another significant deficiency of Articles 1593 and 1596 of the RF Criminal Code while comparing them with Art. 159 of the RF Criminal Code and especially with paragraph "g" of part 3 of article 158 of the RF Criminal Code is deviation from consistent and fair regulation of punishment in the sanctions of these norms.

So, sanction of part 1 of Art. 159 of the RF Criminal Code provides for up to two years of imprisonment as the most severe form of punishment. Sanction of part 3 of Art.158 of the RF Criminal Code provides up to six years, sanction of part 1 of Art. 1593 of the RF Criminal Code provides up to three years, while sanction of part 1 of article 1596 of the RF Criminal Code does not entail imprisonment at all and indicates punishment in the form of hard labour, which cannot be applied because the court is entitled to impose it only as alternatives to imprisonment as follows from Article 531 of the RF Criminal Code. We consider that this incoherence in assessing the level of social danger of related crimes requires attention of the legislator.

Thus, the regulation of criminal law protection of social relations in the digital economy field needs improvement. It should be designed on the basis of narrowly focused and complex natured scientific developments that consider countering relevant crimes in terms of mutual influence of economic and criminal activities, as well as the use of the rapidly developing information and communication technologies in their implementation.

REFERENCES

[1] V.M. Aliyev, N.N. Solovykh, Digital economy oblige us to solve the problem of digital sovereignty securing, Security of Business. No 3, 2018. P. 18-22. (in Russian)

[2] N.S. Bogacheva, B.A. Spasennikov, Issues of crime prevention in the digital economy field, On the way to a civil society. No 3 2017. P. 17-21. (in Russian)

[3] V.A. Vaipan, Digital Economy Legal Regulation, Entrepreneurial law, "Law and Business" Appendix. No 1, 2018. P. 12-17. (in Russian)

[4] D.H. Valeyev, A.G. Nuriyev Russian Justice in the Digital Economy Realities, Civil and Arbitration Proceedings. No 5, 2019. P. 3-8. (in Russian)

[5] S.V. Ivantsov, B.A. Spasennikov, S.V. Borisov, Crime Prevention Problems in the Digital Economy Field,Major aspects of science and education. No 2, 2017. P. 20-24. (in Russian)

[6] R.S. Kasymov, Monopolization Control in the Digital Economy Conditions, Competitive law. No 4, 2019. P. 27-30. (in Russian)

[7] M.G. Reshnyak, On Some Issues of Crimes in the Field of High Information Technologies Enforcement, Preliminary Investigation Bodies' Activities Problems and Ways to Resolve them in Russia. Stavropol: SEQUOYIA, 2017. P. 182-189. (in Russian)

[8] A.P. Sukhodolov, S.V. Ivantsov, S.V. Borisov, B.A. Spasennikov, Major aspects of preventing economic crime committed with use of the data telecommunication networks, Russian journal of criminology. No 1. Vol. 11, 2017. P. 13-21. (in Russian)

[9] R. Broadhurst, P. Grabosky, M. Alazab, S. Chon, Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime, International Journal of Cyber Criminology. Vol 8, Issue 1, 2014, pp. 1-20.

[10] E. Brousseau, N. Curien, Internet and Digital Economics: Principles, Methods and Applications. Cambridge University Press, 2008. 822 p.