HELIX
The Scientific Explorer

DOI 10.29042/2019-5458-5461

Helix Vol. 9 (5): 5458- 5461

Study of Russian and the UK Legislations in Combating Digital Crimes

[1]Alexandra Yu. Bokovnya, [2]Zarina I. Khisamova, [3]Ildar R. Begishev
[1]Kazan Federal University, Ph. D. in Law, Faculty of Law, Criminal law Department
[2]Department of Planning and Coordination of Research Activities, Ph. D. in Law, Head, Research Department, Krasnodar University of the Ministry of Internal Affairs of the Russian Federation
[3]Kazan Innovative University named after V. G. Timiryasov (IEML), Ph. D. in Law, Honored Lawyer of the Republic of Tatarstan, Senior Researcher
Email: at240886@gmail.com, alise89@inbox.ru, begishev@mail.ru

Received: 20th August 2019, Accepted: 30th September 2019, Published: 31st October 2019

Abstract
The purpose of this article is to formulate proposals to improve the criminal law of the Russian Federation on liability for digital crimes on the basis of a comparative legal study of the UK legislation in this area. The work provides a detailed comparative legal analysis of the UK legislation in the field of combating digital crimes. Based on the study, we proposed some mechanisms for ensuring the security of relations in the digital field.
The cross-border nature of these attacks among the main tasks includes unification of legal norms governing the IT sphere, creation of a single mechanism to hold accountable for attacks in the IT sphere worldwide, regardless of geopolitical boundaries. A separate direction of the internal criminal policy of all countries shall be the creation of effective mechanisms for applying the provisions of legislation in the digital sphere; any legislation, even the most progressive, is useless and only declarative in nature without the necessary mechanism for its application. Evidence of the person's guilt is required in order to prosecute. The informational nature of infringements necessitates expanding the boundaries of the powers of law enforcement agencies, which inextricably leads to the problem of finding a balance between observing the freedoms of citizens in the information space and ensuring the universal information security. In the UK, as in all countries of the world, the answer to this question has not yet been found.

Keywords
Digital Information, Digital Economy, Critical Infrastructure, Unauthorized Access, Criminal Law, Crime, Liability, Criminal Liability, Cybercrime

Introduction

Transition from a production to a digital model of the economy has covered almost the entire world community. There is a widespread adoption of technologies for storing big data, digitalization of the banking sector, healthcare and education systems, and other industries. It is only natural that the widespread adoption of digital technologies is directly dependent on the prevalence of their use for illegal purposes. The legislative acts that outlaw certain types of activities are being developed to prevent the growing threat and minimize the existing consequences. The UK experience as the most “digital” country in the world in combating crimes committed using digital technologies seems to be needed and relevant as never before. Today, the country has transformed into a leading global digital economy. The UK has the most productive scientific base, and ranks first in many key global indicators of research quality.

Materials and Methods

The work materials included the provisions of the criminal and information laws of the UK and Russia, as well as the legal acts in the field of ensuring the security of relations in digital sphere.
The reliability of results obtained is ensured based on the analysis of significant and necessary array of legislative norms, statistical data, as well as the use of modern research methods of legal institutions: historical and legal, logical, formal-legal, comparative law, system-structural and other methods of scientific knowledge.

Results and Discussion

According to the study made by the Boston Consulting Group (BCG), an international management consulting company, the UK is the leader in the share of the digital economy in the country's GDP. The area, which includes information technology and telecommunications, government costs related to the Internet, cybersecurity takes the second place in the country's economy - about 12.4%, and seconds only to real estate, and at the same time overtakes trade and production [1]. The country is in the TOP 5 of countries with developed digital economies (Digital Evolution Index 2017) [2], innovation development index (the Global Innovation Index 2017) [3], international index of digital economy and society (I-DESI) and information and communication technology development index (the ICT Development Index 2017) [4].
On March 1, 2017, the UK adopted the UK Digital Economy Strategy 2017 [5]. The main goal of adopting the Strategy is to create, after leaving the EU, an economy that is resilient to changes and suitable for the future. It is noted that the UK has always been at the forefront of digital innovation: from the very first days of the invention of computer technology to the development of the World Wide Web. The Strategy identifies 7 priority areas:
- creation of a world-class digital infrastructure;

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

- formation of digital skills and inclusiveness;
- creation of favorable conditions for the start and development of digital business;
- creation of conditions for conducting digital business by small and medium-sized enterprises;
- preservation by the government of world leadership in servicing its citizens on the Internet (digital government);
- creation of conditions for an open data policy and increase of public confidence in its use;
- ensuring security and secure cyberspace.

To achieve these goals, the Digital Economy Act 2017 was adopted on April 27, 2017 [6]. The law regulates in detail and discloses the content of concepts in the field of providing access to digital services; makes amendments to the rules governing the operation and development of digital infrastructure and digital government; introduces restrictions aimed at counteracting the spread of pornography involving minors on the Internet, as well as protecting intellectual property.

An analogue of the law under consideration is the program "Digital Economy of the Russian Federation" adopted in Russia [7], which was subsequently transformed into the national program of the same name, adopted in accordance with the Decree of the President of the Russian Federation No. 204 dated May 7, 2018 “On National Goals and Strategic Tasks of the Development of the Russian Federation for the Period until 2024” [8] and approved by the Presidium of the Council under the President of the Russian Federation for Strategic Development and National Projects of the Russian Federation, protocol No. 16 dated December 24, 2018.

The most significant contribution to the digital transformation of the Russian economy is made by the implementation of the national program “Digital Economy of the Russian Federation”, which includes 6 priority areas:

- normative regulation of the digital environment;
- information infrastructure;
- personnel for the digital economy;
- information security;
- digital technologies;
- digital government.

Particular attention in the Russian national program is paid to the security of the CII, and the introduction of digital technologies, in particular, new intelligent technologies, since the formation of legal basis for the use of artificial intelligence has begun, which requires taking actions and decisions to prevent possible negative manifestations of its use and state response to them [9-11].

The most important issue for the digital economy is the application and use of IoT technologies. Thus, for example, R. Woodhead, P. Stevenson and D. Morrie point out that the ecosystem perspective shall influence the IT strategy, since the emerging “digital layer” goes beyond the boundaries of the smart city and continues to function long after completion of the traditional construction project [12].

However, despite the measures taken, according to M. Hewlett, director of operations at the British National Cybercrime Administration, “about half of all recorded crimes in the UK were somehow related to cybersecurity” (56% or 1.9 million) in 2017 [13]. At the same time, about 68% of large British enterprises also detected cyber security breaches or attempted attacks in the last 12 months [14]. The question remains open.

G. Horsman notes that, despite the fact that law enforcement agencies are currently combating digital crime, the question still arises as to whether they can maintain this level in the context of rapid spread of digital crime [15], including in the face of threats to information security in the UK after brexit [16].

In the light of development of the digital economy, some suggestions are made to improve the quality of digital forensics, based on the experience and more established practice of other judicial disciplines [17].

According to the UK National Statistics Agency, 367,845 reports of digital fraud (an increase of 11% against APPG), and 13,357 computer crimes were recorded as of September 2018 [18]. For comparison, according to the official statistics of the Ministry of Internal Affairs of Russia, 95,876 digital frauds (4.4% of all crimes recorded in Russia, an increase to 37% against APPG) and 2,499 computer information crimes were registered in the Russian Federation for 2018 [19]; the damage amounted to about 400 billion roubles in Russia, while it is estimated at about 84 billion roubles in the UK. Thus, we can conclude that the damage to citizens and organizations from criminal offenses is 5 times higher in Russia than the same damage to British nationals, while the total number of attacks recorded in the Russian Federation is significantly lower than the UK official criminal statistics. This circumstance can be explained by the high latency of digital crimes in the Russian Federation [20].

In order to establish the UK as a safe and secure cyberspace, the National Cybersecurity Strategy 2016-2021 was published on November 1, 2016 [21]. The main objective of the Strategy is the achievement by the UK of the status of a safe and resilient to cyber threats, prosperous and confident country in the digital world by 2021.

A similar strategic document is available in Russia - the Doctrine of Information Security of the Russian Federation [22]. It defines strategic goals and the main directions of ensuring information security, analyzes the main information threats and assesses the state of information security.

In the UK, the main law governing liability for crimes, involving the use of information and telecommunication technologies, is the Computer Misuse Act 1990 [23]. At the end of the last century, the law became a kind of “reaction” to the growing alarm in society that the laws that existed at that time were not commensurate with the threat to society, emanating from hackers [24].

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

Problems of development of the UK legislation in the IT field are considered in detail in the special information sources [25].

Let us consider in more detail the provisions of the Law on Unlawful Use of Computer, the provisions of which were repeatedly subjected to significant adjustments.

Section 1 of the Law provides for punishment for unauthorized access to computer materials. This norm can be considered as a fundamental crime, since it often precedes the commission of other, more serious crimes. The crime is considered completed from the moment the person turned on the computer to obtain the authorized materials. It does not matter how much he/she has managed to implement his/her intent. The norm is general, therefore the attacker's intent shall not be directed to any specific information, data or program stored on the computer

Access is unauthorized if the person does not have the right or has not received consent to such access. The understanding by the UK legislation enforcer of the content of unauthorized access is similar to that given in the European Convention for the Suppression of Cybercrime [26].

It is necessary to answer that officials, who exceed the limits of their authority to access information, to which they were not admitted, also fall under this rule.

Section 2 of this Law stipulates the liability for unauthorized access with an aim of committing or facilitating the commission of new crimes. Such access is also a preparatory stage in the commission of another (new) crime. A person may be convicted of a crime, even if the commission of a basic crime is impossible (Part 4 of Art. 2). A person found not guilty under Art. 2 or 3 of the Law by a jury, may be convicted of a crime under Art. 1.

Section 3 of the Law provides for liability for unauthorized actions with respect to computer systems with an aim of causing damage or through negligence. A person is convicted of a crime if he/she commits any unauthorized action, including gaining access to data. Those quilty in DDoS attacks are also imposed responsibility under Art. 3.

Article 3ZA provides for liability for unauthorized actions that cause or create the risk of serious damage.

The specified norm is aimed at suppressing attacks on objects of critical national infrastructure (depending on the performer's motives, anti-terrorism legislation can also be applied). We believe that the norm under consideration is identical in essence to Art. 274.1. of the Criminal Code of the Russian Federation.

Conclusions

The following should be noted in the summary. A fairly coherent system for ensuring the security of relations in the digital sphere has been created in the UK today; the country has adopted and successfully applies the criminal law in this area. In our opinion, the casuistic nature of Anglo-Saxon law and its flexibility have a particular advantage in the face of constant transformation and changes in legal relations in the digital sphere. However, the conducted comparative analysis allows making a conclusion that the provisions of the Russian criminal law, as well as the British one, reflect an adequate reaction to the emerging criminal assaults.

However, in the conditions of continuous improvement of digital technologies and their quick adaptation for criminal purposes, we consider it appropriate to create more universal standards in Russian legislation with a certain “strength threshold” for new types of threats.

Summary

At the same time, in the context of globalization for all countries, it becomes obvious that crime in the IT sphere is an integral part of the digital economy, because, as we know, either side has two medals. And with a greater informatization of society, its borders will grow, gradually completely replacing traditional crime. And it is necessary to respond to it comprehensively and constantly.

Acknowledgements

The work is performed according to the Russian Government Program of Competitive Growth of Kazan Federal University.

The authors are sincerely grateful to the head of the Department of Criminal Law of the Faculty of Law of the Kazan Federal University for help in the preparation of this article.

References

1. The Boston Consulting Group (BCG). – URL: https://www.bcg.com/ru-ru/default.aspx
2. TOP 10 countries with the most developed digital economy.URL: http://web-payment.ru/article/250/top-10-cifrovaya-/
3. Cornell University: The Global Innovation Index 2017. – URL: https://gtmarket.ru/ratings/global-innovation-index/info#united-kingdom
4. International Telecommunication Union: The ICT Development Index 2017. – URL: https://gtmarket.ru/ratings/ict-development-index/ict-development-index-info#united-kingdom
5. UK Digital Strategy 2017. – URL: https://www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy#a-safe-and-secure-cyberspace-making-the-uk-the-safest-place-in-the-world-to-live-and-work-online
6. Digital Economy Act 2017. – URL: https:// http://www.wipo.int/wipolex/ru/text.jsp?file_id=474843

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

7. Decree of the Government of the Russian Federation No. 1632-r dated July 28, 2017 “On approval of the program “Digital Economy of the Russian Federation” // Official Gazette of the Russian Federation. – 2017. – No. 32. – Art. 5138.
8. Decree of the President of the Russian Federation No. 204 dated May 7, 2018 “On National Goals and Strategic Tasks of the Development of the Russian Federation for the Period until 2024” // Official Gazette of the Russian Federation. – 2018. – No. 20. – Art. 2817.
9. Khisamova Z.I., Begishev I.R. Legal Regulation of Artificial Intelligence / Z.I. Khisamova, I.R. Begishev // Baikal Research Journal – 2019. – V. 10, No. 2. DOI: 10.17150/2411-6262.2019.10(2).19.
10. Begishev I.R., Khisamova Z.I. Criminological risks of using artificial intelligence / I.R. Begishev, Z.I. Khisamova // Russian Journal of Criminology. – 2018. – V. 12, No. 6. – P. 767-775. DOI: 10.17150/2500-4255.2018.12(6).767-775.
11. Khisamova Z.I., Begishev I.R. Criminal liability and artificial intelligence: theoretical and applied aspects / Z.I. Khisamova, I.R. Begishev // Russian Journal of Criminology. – 2019. – V. 13, No. 4. – P. 564-574. DOI: 10.17150/2500-4255.2019.13(4).564-574.
12. Woodhead R., Stephenson P., Morrey D. Digital construction: From point solutions to IoT ecosystem / R. Woodhead, P. Stephenson, D. Morrey // Automation in Construction. – 2018. – № 93. – P. 35–46.
13. Crime in England and Wales: Additional tables on fraud and cybercrime. – URL: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesexperimentaltables
14. Cybercrime in the UK. – URL: https://www.governmenteuropa.eu/cybercrime-uk/86105/
15. Horsman G. Can we continue to effectively police digital crime? / G. Horsman // Science & Justice. – 2017. – № 6 (57). – P. 448–454.
16. Hert P. Vagelis Papakonstantinou The rich UK contribution to the field of EU data protection: Let's not go for «third country» status after Brexit / P. Hert // Computer Law & Security Review. – 2017. – № 3 (33). – P. 354–360.
17. Page H., Horsman G., Sarna A., Foster J. A review of quality procedures in the UK forensic sciences: What can the field of digital forensics learn? / H. Page, G. Horsman, A. Sarna, J. Foster // Science & Justice. – 2019. – № 1 (59). – P. 83–92.
18. National Fraud profile: National Fraud Intelligence Bureau. – URL: https://www.gov.uk/government/organisations/national-fraud-authority/about
19. The official statistics of the Main Information and Analysis Center of the Ministry of Internal Affairs of Russia: form 615.
20. Vorotnikov V.L. Criminal law policy in relation to crimes in the field of computer information / V.L. Vorotnikov // Bulletin of TGU. – 2009. – No. 4 (72). – P. 280-281.
21. National Cyber Security Strategy 2016 to 2021. – URL: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021
22. Decree of the President of the Russian Federation No. 646 dated December 5, 2016 “On approval of the doctrine of information security of the Russian Federation” // Official Gazette of the Russian Federation. – 2016. – No. 50. – Art. 7074.
23. Computer Misuse Act. – URL: https://www.cps.gov.uk/legal-guidance/computer-misuse
24. Emm D. Cybercrime and law. – URL: http://www.crime-research.ru/articles/depo24
25. Kemp R. IT law in the UK: Looking back on 2007 and ahead to 2009 / R. Kemp // Computer Law & Security Review. – 2008. – № 6 (24). – P. 473-474.
26. Convention on Cybercrime (ETS № 185). – URL: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495