УДК 340.115.7

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЗАКОНОДАТЕЛЬСТВА О ЗАЩИТЕ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА В РЕСПУБЛИКЕ КОРЕЯ И РОССИЙСКОЙ ФЕДЕРАЦИИ

Ом Ю Джон,
Магистр 2 курса Юридической школы
Дальневосточного федерального университета,
Россия, г. Владивосток,
Доктор права Юридической школы
Национального университета Чхонбук,
Республика Корея
yoojeong.eom@gmail.com

Научный руководитель:
Иванов Александр Михайлович
канд. юрид. наук, доцент кафедры теории и истории
государства и права Юридической школы
Дальневосточного федерального университета,
г. Владивосток
Ami_25.07@bk.ru

A COMPARATIVE ANALYSIS ON CYBER SECURITY LAW BETWEEN REPUBLIC OF KOREA AND RUSSIAN FEDERATION

Yoo Jeong Eom

2nd year master's student of the Law School
of the Far Eastern Federal University
Russia, Vladivostok,
Juris Doctor of the Law School
of the Jeonbuk National University,
Republic of Korea

Aleksandr M. Ivanov
Dr. of Law, Associate Professor
of the Chair of Theory & History of State and Law,
Law School of FEFU,
Russia, Vladivostok

АННОТАЦИЯ

Бурное развитие информационной индустрии влечет за собой необходимость надлежащего регулирования информационного пространства во всех странах. В данной статье предлагается краткий обзор развития норм в Республике Корея и в России, затрагиваются проблемы, связанные с этим и возможные перспективы их разрешения в будущем.

ABSTRACT

Highly rapid development of information industry has been involved a necessity to a proper regulation of information space in all countries. The following article proposes a short review of development of norms in Republic of Korea and in Russia, takes into consideration some problems connected with it and possible perspectives in their solution in future.

Ключевые слова: сравнительное право; правовая система; информационное пространство; информационная безопасность; правовая политика.

Key words: comparative law; legal system; cyberspace; information / cyber security; legal policy.

1. Introduction

As computer system and information industry have been in a rapid improvement recently, the legislations and legal systems related to computer and information are also undergoing some developments. While the field of data science is being integrated and researched with many different academic areas, Cyber Security is specially on the rise. The following contents of this article will make comparisons between the

developmental process, current legislative systems, and future trends of Cyber Security Law between Republic of Korea and Russian Federation, by taking a look into systems of each country and measuring one against the other. The whole work will then make an overall summary and draw a conclusion in the end.

2. Development Process of Cyber Security Law

A. Cases of Republic of Korea

Since computer networks and information systems are taking huge portions in daily lives, the number of cyber-attacks has also increased, and the society of Republic of Korea is also exposed to the threats caused by Democratic People's Republic of Korea. Proper legislations and national plans are vital to respond domestic and international cyber-attacks, and there have been several laws and policies as results of the efforts to protect the nation in Republic of Korea.

The government of Republic of Korea has enacted *Critical Information Infrastructure Protection Act* since 2002, under the necessity of protecting Critical Information Infrastructure (CII) from cyber-attacks in National Security **[4]**. The Act has made national structure to protect CII from cyber-attacks and described the provisions on designation on CII, evaluating vulnerabilities and establishing protection plans, responding cyber incidents, and penalties. **[11]**

Also, in order to enhance National Cyber Security, Korean policy makers and legislators went through lots of hearings and *Cyber Security Industry Enhancement Act* was newly enacted – the Act enables Korean central and local government, and municipals to establish and perform policies to encourage cyber security industry and prepare measures to allocate budgets to fulfill that policies.

The National Assembly members proposed a bill to independently and wholly focusing on personal information protection, and the bill enacted to be an Act at March 29, 2011 and has been put into effect since September 30, 2011. The Act deals with the responsibilities of personal information managers and the relevant government ministers.

B. Cases of Russian Federation

The laws related to data protection and privacy in Russia have become a rapidly developing branch in Russian legislation, which have mostly been enacted in the 2005 and 2006. *The Russian Federal Law on Personal Data (No. 152-FZ),* which was implemented on July 27, 2006, constitutes the backbone of Russian privacy laws and requires data operators to take "all the necessary organizational and technical measures required for protecting personal data against unlawful or accidental access". **[3]** Russia's Federal Service for Supervision of Communications, Information Technology and Mass Media is the government agency tasked with overseeing compliance.

The basic rule is that the consent of the individual is required for processing of his personal data; yet this rule does not apply where such processing is necessary for performance of the contract, to which an individual is a party. The stance of Federal Service on Telecommunications, the governmental body responsible for personal data protection, had been that adequate and sufficient protection exists only among those foreign states which signed and ratified Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, with three major exceptions permitting transfer of personal data to the countries where lower or no standard of personal data protection applies. The limits on the export of data became stricter as a new "Article 18(5)" came into effect on September 1, 2015.

The Russian legislation imposes strict limitations on direct marketing, processing, and management of data. Relevant provisions require effective protection of personal data, and mandatory regulations on protection of such data have been in development by Federal Security Service to be issued. The regulations provide for protection of all personal data being transferred outside Russia in form of encryption, which are expected to allow the use of only Russian encrypted software and equipment.

C. Comparison

Since modern technology is under rapid changes and developments, legislations in both countries are also undergoing changes recently, by focusing on following up

the changes in society and technology. However, the differences come from the different situations that each nation is facing: Since Republic of Korea is under armistice and cannot exclude the risk of cyber-attacks from the North Korea, it also considers the possible offense and preventions in the process of legislation. Meanwhile, due to the socialistic characteristic of political and system, the governmental bodies in Russian Federation focus on the control of citizens, yet it could bring up some constitutional issues.

3. Current System in the field of Cyber Security Law

A. Overview

As the term 'Cyber Security' indicates, Cyber Security Law is primarily related with secure protection of the rights of individuals from their infringements and prevention on crimes related to cyberspace. The following parts of the article will mainly focus on the criminal regulations and sanctions regarding cybercrime from Republic of Korea and Russian Federation.

B. Cases of Republic of Korea

i. Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.

Republic of Korea has a special legislation for dealing with the deeds occurring in the cyberspace, which is named *Act on Promotion of Information and Communications Network Utilization and Information Protection, etc*. **[4]** This Act regulates promotion of utilization of information and communications network, protection of personal information, protection of personal users, telecommunication and billing services *(Article 1)*; and it separates chapter for penalty provisions on Chapter 10, which specifically impose criminal sanctions on illegal actions or violation of the regulations stated in the Act. Also, since particularly enacted, this legislation of Republic of Korea handles a wider range of occurrence in the sphere of computer information, more than the bounds of criminal law, with additional chapters and articles.

Korean legislation on information and communications network also imposes

criminal sanctions on *(i) unlawful intrusion on information and communications network (Articles 48(1) and 71)*, *(ii) mutilation, destruction, alteration or forge of an information and communications system, data, program or similar (Articles 48(2) and 70-2)*, and *(iii) interference with operation of the information and communications network (Articles 48(3) and 71)*.

ii. Several Articles from the Criminal Code of Republic of Korea

While previously mentioned *Acts on Promotion of Information and Communications Network Utilization and Information Protection, etc.* functions as a special law, several articles are also dispersed in some parts of Korean Criminal Law.

Article 314 of Criminal Code of Republic of Korea prohibits obstructing business by using computer and data processing units; *Article 347-2* directly stipulates punishments on entering false information or improper order by using computer and any kinds of data processor. Some additional articles *(Articles 140(3), 141(1), 227-2 through 229, 232-2 and 234, 316(2), 323, and 366)* respectively regulate crimes related to concealment of official secrecy, damaging of public official documents, forging and illegal use of public and private documents, violation of secrecy, obstruction of others' exercising of rights, and destruction of property, when the means with computer or electronic devices were used. **[2]**

C. Cases of Russian Federation

i. Chapter 28 from the Criminal Code of Russian Federation

The field of computer information crimes are introduced into special Chapter 28 from the Criminal Code of the Russian Federation. **[1]** The articles included in this chapter of Russian Criminal Code deals with the crimes in the sphere of computer information, as the title of the chapter suggests. Three legislative articles regulate criminal liability on *illegal access to computer information (Article 272)*, *creation, use and distribution of malicious computer program (Article 273)*, and *violation of the rules of operation of the storage means, processing or transmission of computer and information and telecommunications networks (Article 274)*. According to the newly

added article, *unlawful impact upon the crucial information infrastructure of the Russian Federation (Article 274.1)* is also punishable.

ii. Additional Penalty Clauses related to the Cyber Security

While a separate chapter is established along with the development of information system in order to control computer crimes, several computer crimes related with fraud were included in *Article 159.3 and 159.6* from Chapter 21 of the Criminal Code, which deals with Crime against Property. **[1]**

The additional articles prohibit swindling through the use of electronic payment means and swindling in respect of computer information; the reason that the articles are separated from the chapter is supposed as the higher relation of the articles to the economic nature of the deeds being regulated.

D. Comparison

While the Criminal Code of Russian Federation specifically stipulates the rules regarding computer and information crimes in Chapter 28, In Republic of Korea the criminal provisions in the field of computer and information are specially regulated by a particular law named *Act on Promotion of Information and Communications Network Utilization and Information Protection, etc*.

Both provisions of Russian Federation and Republic of Korea share some common scope of regulation. Both countries impose penalties on *illegal access to computer information (Article 272 in RF; Articles 48(1) and 71 in ROK)*, *creation, use, and dissemination of harmful computer program (Article 273 in RF; Articles 48(2) and 70-2 in ROK)*, and *violating rules for operation of the facilities for computer information storage, processing and transmittance and of information-telecommunication networks (Article 274 in RF; Articles 48(3) and 71 in ROK)*. The additional articles on Criminal Code which regulates swindling through electronic devices also share similarities.

The differences of each country are that the punishments in Republic of Korea is maximum five to seven years *(Articles 70-2 and 71)*, while Russian Federation

imposes similar punishments only when the deeds have entailed heavy consequences or a threat of their occurrence. Both countries also show differences in that Russian Federation has special chapter for computer information crimes within the Criminal Code, while Republic of Korea has a specific law and criminal provisions for similar crimes; thus, Korean law regulate a bit wider range of deeds occurring in the cyberspace. Also, there are no criminal sanctions in Republic of Korea which corresponds to *Article 274.1* of the Criminal Code of Russian Federation, which seems to be a result coming from the difference in social structure and political system between two countries.

4. Newly Established Legislations and Expected Trend of Changes

A. Overview

Countries all over the world are showing large and small movements in order to follow up the rapid changes of information and technology. Considering the role of legislations to protect human rights and duties and control the society, changes in regulations are essential as well. The following paragraphs will describe the major changes and trends that would appear in the near future in Republic of Korea and Russian Federation respectively and make comparisons.

B. Cases of Republic of Korea

i. Data Protection Laws

Amendments on Data Protection Laws were passed in a regular session of National Assembly of Republic of Korea on January 9, 2020. Three main Data Protection Laws include *The Personal Information Protection Act (PIPA)***[4]**, *Act on Promotion of Information and Communications Network Utilization and Information Protection, etc*., and *Credit Information Use and Protection Act*.

Fostering “new” industries via active use of data is regarded as main national task in Republic of Korea, along with the Fourth Industrial Revolution. More specifically, the use of data with applying new technologies such as Artificial Intelligence, Clouds, and Internet of Things are necessary; thus, establishing the social

norms are urgent and indispensable. The amendments mainly cover introducing the notion of pseudonymous data, efficiency of governance system on protecting personal information, strengthening the responsibility of personal information manager, and specifying the ambiguous criteria of defining 'personal information'.

C. Cases of Russian Federation

i. Russian Internet Law

Russia has passed the sovereign internet law giving it the right to cut the Russian part of the Internet off from the rest of the online world in November 2019. This law provides stable operation of the Russian Internet (RuNet) in case it is disconnected from the global infrastructure of the World Wide Web. **[3; 5; 13;14]**

While the law was expected to provide for central control of internet traffic and remove the need for data to be sent to and received from foreign servers, the control also accompanied with worries on traffic monitoring and stark censorship of sites visited by Russian users. This law seemed to be welcomed by several domestic companies and providers; yet concerns from overseas also followed – bringing the prediction of going after China's path and controversies on security versus censorship. **[12]**

D. Comparison

While future legislations of two countries mainly deal with computer and internet as information technology is the mainstream technique nowadays, the biggest difference is that Republic of Korea is more focusing on protection of individuals' rights and information and restriction of possible infringements, while Russian Federation concentrates on social regulation and independent provision of technique, in spite of concerns on censorship issues and global isolation.

5. Conclusion

In conclusion, Russian Federation regulates computer information crimes in a special chapter 28 in its Criminal Code, in addition to pre-existing several crimes with

computer that are related to the property. The criminal legislation of Russian Federation also shows some distinctiveness compared to other Anglo-American and European countries, and it also has some common and different aspects when compared to the law on computer information and networks of Republic of Korea. Although they share similar scope of regulation in common, the ways and forms of regulation and the degree of punishments differ from each other. Considering the increasing number of cybercrimes, the legislator needs to take a more proactive stance, in order to protect the social interest and the state from cyber threats, as mentioned in the article.

References:

1. Criminal Code of Republic of Korea // URL: https://www.refworld.org/docid/3f49e3ed4.html (accessed 27.06.2020)
2. Criminal Code of Russian Federation // URL: https://www.wipo.int/edocs/lexdocs/laws/en/ru/ru080en.pdf (accessed 27.06.2020)
3. "Data Protection (Privacy) Laws in Russia." // URL: https://pd.rkn.gov.ru/authority/p146/p164/ (accessed 27.06.2020)
4. "Data Protection in South Korea: Why You Need to Pay Attention." International Expansion and Global Growth Experts, 11 June 2015, URL: ieglobal.vistra.com/blog/2018/8/data-protection-south-korea-why-you-need-pay-attention. URL: https://www.privacy.go.kr/eng/laws_policies_list.do (accessed 27.06.2020)
5. Doffman, Zak. Putin Signs 'Russian Internet Law' To Disconnect Russia From The World Wide Web. // Forbes, Forbes Magazine, 1 May 2019, URL: www.forbes.com/sites/zakdoffman/2019/05/01/putin-signs-russian-internet-law-to-disconnect-the-country-from-the-world-wide-web/#56825ac71bf1.
6. Evdokimov, K.N. Comparative Study of Criminal Legislation of Russia and Foreign Countries Providing for Liability for Committing Computer Crimes. // European Journal of Law and Political Sciences, Dec. 2017, pp. 10–13., doi:10.20534/ejlps-17-4-10-13.
7. Khayryuzov, Vyacheslav. Privacy And Cybersecurity In Russia - Privacy - Russian

Federation.// Articles on All Regions Including Law, Accountancy, Management Consultancy Issues, Noerr, 31 Oct. 2018, URL: www.mondaq.com/russianfederation/Privacy/750216/Privacy-And-Cybersecurity-In-Russia.

8. Kshetri, Nir. Cybercrimes in the Former Soviet Union and Central and Eastern Europe: Current Status and Key Drivers. // Crime, Law and Social Change, vol. 59, no. 2, 21 Mar. 2013.
9. Lindenau, Jan. Will Russia Enforce Its New Internet Laws in 2020? // The Moscow Times, The Moscow Times, 31 Mar. 2020, URL: www.themoscowtimes.com/2020/01/03/will-russia-enforce-new-internet-laws-i2020-a68802.
10. Nikkarila, Juha-Peka, and Mari Ristolainen. 'RuNet 2020' - Deploying Traditional Elements of Combat Power in Cyberspace? // Conference Paper, May 2017.
11. Park, Kwang Dong, et al. Introduction to Korean Cyber Security Law. // International Legal Collaboration Research, vol. 16, no. 18.
12. Rodgers, James. Russia's New Internet Law: Security Or Censorship? // Forbes, Forbes Magazine, 17 Apr. 2019, URL: www.forbes.com/sites/jamesrodgerseurope/2019/04/17/russias-new-internet-law-security-or-censorship/#2273666674a4.
13. Russia Internet: Law Introducing New Controls Comes into Force. BBC News, BBC, 1 Nov. 2019, URL: www.bbc.com/news/world-europe-50259597.
14. Sukharenko, Alexander N. Russian ITC Security Policy and Cybercrime. // PONARS Eurasia Policy Memo No. 601, July 2019.