Advances in Economics, Business and Management Research, volume 81
1st International Scientific Conference "Modern Management Trends and the Digital Economy: from Regional Development to Global Economic Growth" (MTDE 2019)

Digital safety as a factor of domestic and international policy: legal and social aspects of the problem

Pryadko I.P.
Moscow State University of Civil Engineering (MGSU)
Moscow, Russia
Pryadcko.igor2011@yandex.ru

***Abstract* — The author analyzes the actions taken within the framework of the legal and political governance in the area of information security. The author believes that within the last five or six years this issue turned highly politicized; therefore, today its resolution requires both legal and political methods. The author acknowledges the need to strengthen domestic and international actions employed to govern political and legal relations in the area of intellectual property and its protection, to restrict access to any confidential information. The author discusses the safety of information and telecommunication systems and demonstrates the influence of information safety on business and management activities. The author offers his analysis of the Federal laws "On trade secrets" and "On personal data", etc. The author also assesses the political damage inflicted by international organized crime in the infosphere.**

Keywords — information safety, legal regulation of information, information technologies, law on computer-generated signature, economic safety, infowar, Snowden, informatization

I. INTRODUCTION

It is most likely that the need to safeguard information arose concurrently with the appearance of *homo sapiens* as a species, as the latter has a flexible and multi-tier system of signs, or a natural language. As early as in the Bronze Age, when written cultures were in the process of their inception, there arose a need to communicate information. Notably, in a class-divided society, this mission was assumed by a special social category of people – priests, who zealously safeguarded the crumbs of knowledge that they had obtained. In the course of thousands of years, the written culture developed from wedge writing, or inscriptions made on clay tablets, into advanced data storage facilities. Needless to say that as the time progressed, the nature of any valuable information, as well as information leakage patterns, transformed. However, in the present-day postindustrial society (the information society, the technotronic society, or "the third wave" society, as it was called by A. Toffler [1], a futurist and a social thinker), information has accrued value. Information technologies are being systemically and orderly introduced into politics, entrepreneurship, law enforcement activities, social performance, federal/municipal governance, urban economy and other life spheres [2]. However the confrontation between information holders and those willing to capture it remains. Nowadays the problem of digital terrorism (or cyber-terrorism) has obtained the status of a global threat to our civilization. It is no accident that the accelerated assimilation of digital technologies, particularly, in the area of politics, causes natural concerns. Large-scale informatization and computerization has quite a few drawbacks along with strengths.

The introduction of advanced information technologies, conversion to electronic carriers, capable of accumulating enormous amounts of information, multiply the importance of information security for all those who are engaged in civil transactions (including subjects of economic activities operating on competitive markets), and for the political life. Gordon Moore's law saying that the number of transistors in a dense integrated circuit doubles about every two years has not been working for a long time [3, 4]. Computers get to process larger amounts of information a lot faster than it was projected by this IT researcher. The information flow has multiplied manifold, let alone the pace of development of telecommunications, means of communication, transport, emergence of advanced information carriers, involvement of extensive groups of people into the political life, and democratization of political administration. Against this background, any destruction or unauthorized access to databases, any malfunction in the operation of information systems, including those responsible for the national security, as well as other contingencies may cause (and this is what they usually do) substantial losses, whereas any unlawful acts in the sphere of digital technologies produce immediate effects. However the main point is political and economic damage inflicted: in some cases, the national economy and the political image of the country suffer, in other cases the reputation of some particular organization or firm is under threat. If an organization acts as a subject of international economic activities, it may lose its share of the services/commodities market. In view of these consequences, the author attempts to solve the problem of information security as an integrated issue, because it encompasses law, economy, marketing, information theory, logic, domestic and foreign policies. Some specialists distinguish the information policy [5] from the digital policy, which can be focused on destruction of information safety in competing states. Being limited by the article format, the author has to reduce his efforts to the most significant political and legal aspects of this problem (the application of a computer generated signature, personal data safeguarding, political espionage, etc.). The author also focuses on the domestic factors of financial, economic and

political safety (the procedure of elections into government authorities); the author also considers political and legal problems of trade secrets and their safeguarding by different firms and organizations. These objectives have pre-determined the subject matter and the scope of research implemented in this project, as well as its methods discussed in the next paragraph.

The information security as a most vital need of organizations, specializing in business operations, finance, and state management, represents *the scope of research* covered in this article. Its *subject matter* consists in political and legal actions taken to make sure that the information is secure.

II. METHODS AND METHODOLOGY

The literary sources, used by the author, include the most important and frequently applied regulatory acts on information security. They include the Constitution of the Russian Federation [6], Federal laws "On information, informatization, and information security", "On computer generated signatures", "On archiving in the Russian Federation", "On state secrets" [7], "On trade secrets", "On personal data", "On banks and banking activities" [8], etc. The author has also taken advantage of the theoretical works, focused on research into the structure of the present-day informational culture, the pace of the IT penetration into the contemporary society, and political aspects of informatization. Indeed, the sources that serve as the basis for this article, include the works written by reputable Russian legal experts, political analysts; theoretical works on problems of information law, including those written by K.N. Evdokimov, who is engaged in the study of versatile aspects of computer crimes in our country and worldwide [9], books written by V.P. Melnikov [10], V.A. Kopylov [11], in which their authors study theoretical and political constituents of the information law, articles written by O.L. Soldatkina, in which she considers constituents of the informational policy [5] and several other contemporary Russian and foreign political experts, practicing lawyers and legal theorists. In particular, the author employed several conclusions made by I.V. Bashelkhanov, the general manager of a major project entitled "The Russian Innovative Encyclopedia" implemented by the Federal state budgetary institution of higher education "The Financial University under the Government of the Russian Federation". This researcher attempted to implement an experimental political and legal project: he drafted the digital code of the Russian Federation [2]. This project has absorbed the opinions expressed by the representatives of the civil society, publicists and political experts [12]. I.V. Bashelkhanov analyzes the influence produced by information technologies on the socio-political patterns of the human behaviour to make a conclusion about the accrual of threats in the contemporary society.

On top of such methods as the comparative historic analysis and the look back analysis applied to political and legal sources employed by the author to analyze the application of the information law, the author also takes advantage of mandatory and non-mandatory norms applied in this branch of law. These norms distinguish prohibition from permission. The extent of rigid regulations, which are obligatory for execution under a threat of sanctions (the imperative principle) in the information law are supplemented by the right to choose the behavioural pattern, after having entered into relations governed by the information law (the principle of discretion applied to assure public order). Laws are applied to assure the legal compliance of any relations, arising in respect of information security.

Political and legal methods serve to protect data processing. The legal framework, or effective laws, is pre-determined by the in-depth socio-economic and political changes that have been underway both in the Russian society and in international politics [10]. Here we can mention the restrictions imposed on the operation of Russian media agencies on the information markets of the USA, the prosecution of the software developers, having Russian or Chinese origin, or the origin of other developing nations. Let's remember about the infowars pursued worldwide; the willingness of Russia and several other countries to employ their information resources to overcome the paradigm of the monopolar world and to ensure their national security by means of ensuring their digital security, to maintain their political independence, etc. The country is willing to further its economic development, to generate new types of information services in a digital economy (the so-called Economy 4.0) and to respond to the ever changing environment.

We can define the notion of information safety by distinguishing specific approaches towards the use of information and information resources. Pursuant to these differentiating patterns, criminal offences committed in respect of information resources, can also be grouped. K.N. Evdokimov, a political expert, considers foreign-policy developments as the drivers of IT crimes in our country. "… political and informational drivers of cybercrimes in Russia include the need for intelligence services of foreign states to obtain items of confidential geopolitical, military, technological, financial, economic, diplomatic and strategic information about the Russian Federation" [9].

III. RESULTS

A. The study of political and legal precedents

Let us analyze the provisions of the law "On information, information technologies, and information security" [13]. It defines the notion of information as the subject of political and legal relations; it also provides the definitions of an information system, information technologies, an information holder, information access, and an information telecommunication network. This regulatory act obliges an information holder or an operator of an information system to safeguard the information, namely, to prevent any unauthorized access to information or any impacts on the technical facilities applied to process the information and to be able to immediately restore any damaged political and legal information, as well as to take other actions stipulated by the law. This Federal law establishes the right of citizens to obtain information and prohibits any informational restrictions in respect of any rights, responsibilities and liberties of a man and citizen. Free information/data turnover and assurance of information security are now perceived as the indicators of the society's transparency and maturity of a democratic state.

Many of the aforementioned laws are being comprehensively and purposively applied to regulate versatile branches of economic activities. These legal acts serve as the basis for local normative acts. It is noteworthy that in

particular cases a subject of the law, who must competently store the information obtained in the course of his/her work (for example, a government official or a political leader), violates provisions of Federal laws. Even in our day-to-day activities, we can come across the disclosure of personal and public information. These widely spread cases include the disclosure of the personal information about the holder of a telephone number in the offices of telephone operators, the bribery of telephone operator managers, or the misuse of personal data by bank officers. These examples demonstrate violations of the law "On personal data" [14]. They can be compared with the effect of another Federal law "On business secrets": any customer of a telecommunications company, acting in the capacity of a natural person or a legal entity, enters into an agreement (a business deal) for the provision of mobile communications services by the operator [15]. In this case, the legal framework of information safety immediately turns politicized, if the injured person represents a famous politician or a public organization.

B. The safety of bank and government documents: the challenges of the 21st century

Security assurance actions, applied in finance and economics, are reasonably the same as those used in politics and state governance: the same data protection software is installed onto the hardware of government agencies and banking institutions. Violations of the information laws also have the same origin.

Sometimes the issuance of an electronic document, bearing an approved letterhead, misses a computer-generated signature, which also represents an evident violation of the effective laws of the Russian Federation. M.V. Borodin, a contemporary legal theorist and political expert, makes the following statement in his article: "By virtue of its nature, a computer-generated signature represents an independent element in the structure of an electronic document and confirms the authorship, authenticity and non repudiation of the electronic document's compiler or holder" [16].

The above-mentioned actions are applicable to public documents, namely, to the RF Presidential Decrees or other non-legislative acts, which are regularly published on the official website of the President of the Russian Federation [17]. The same system of actions is applied to the documents, published for business purposes by subjects of domestic civil transactions. Any publications of this kind can be made by the "Bank-Client" banking software, which can assure the confidentiality of any electronic document bearing a computer-generated signature.

It is noteworthy that a substantial threat to the national security arises in the days of domestic political events, which are significant for democratic states, including elections into executive or legislative government authorities. Those who conduct infowars may have forged documents and falsified statistics at their disposal; websites of government authorities and non-governmental organizations may be cracked. Hackers keep making attempts to crack the GAS-Vybory (Elections) software to collect the voting results. Therefore, the software, developed for government authorities, has several security levels. Dark web peer networks can also be employed for criminal purposes. It should be noted that the name of this segment of the world telecom network speaks for itself, as it is frequently used by versatile criminal groups and representatives of the "shadow" economy. Intelligence services of the leading nations (for example, the US navy intelligence) also take advantage of the dark web [19]. Presently, dark web networks are most widely used as a platform for illegitimate operations, drug trafficking, illegal traffic in arms, and, moreover, they serve as the platform for focused actions targeting the sovereignty of the states exposed to cyber attacks. The problem can be solved by improving virus protection programmes.

According to Edward Snowden, a former CIA employee, specialists of the National Security Agency (NSA) had developed the malware which hit the computers all over the world and in Russia, in the May of 2017. The propagation of computer viruses is particularly dangerous for the digital networks of hospitals and social security offices. "Despite warnings, NSA built dangerous attack tools that could target Western software," Mr. Snowden said. "Today we see the cost. If NSA had privately disclosed the flaw used to attack hospitals when they found it, not when they lost it, this may not have happened." The damage inflicted by the attack made by anonymous cyber-criminals in 2017 turned out substantial and reached millions of US dollars. This explains why the draft Digital Code positions digital software applications as a weapon of mass destruction [12]. The damage, produced through the worldwide web, causes economic and socio-psychological consequences.

IV. DISCUSSION

And now let's focus on the issues that comprise the subject of animated discussions of the safe use of digital resources in the socio-economic sphere. Digital security is a must in the area of services (banking services) provision. The reduction of cash payments and the use of different types of electronic money is a global trend. Telecom payment processing networks turn more popular. Against this background, data and information safety turn particularly vital in the banking industry, and financial documents must be safeguarded both from local criminals and international cyber-terrorists striving to obtain illegal access to banking data. It is particularly important to analyze the way the problem of the information confidentiality is resolved by a financial institution, on the one hand, and by a natural person or a legal entity, acting as a consumer of financial services, on the other hand. Whenever a customer enters into an agreement for the installation of the "Bank-Client" software, the parties execute an agreement that encompasses (1) data safeguarding from any encroachments by third parties and (2) a safe data delivery channel to be used by the bank and its customers. In its turn, the bank provides the client with an access code (a login and a password) needed to enter the system. The legal framework governing the security of banking institutions must be tightened to the maximal extent, as cyber attacks multiply every year. The amounts of money, thus stolen, have gone up multifold.

In the beginning of this work we provided examples of digital attacks on items of vital infrastructure. The most vivid example of a negative impact, produced by global digital systems on the economic safety, is a "cash register strike" that occurred in December, 2017. Back then, numerous cash centres collapsed in major cities of Russia and worldwide. The Federal Taxation Service of the Russian Federation got involved to solve the cash register strike problem.

V. CONCLUSIONS

The political and legal analysis of information safety infringements, discussed in this article, serves to conclude that there is a sufficient number of laws and technologies that are needed to assure information safety. Nonetheless, attacks on networks run by private companies and government authorities turn all the more proactive and impudent, and their consequences aggravate. Information security problems are to be resolved at the international scale. Hence, we need advanced IT technologies. Software developers are to develop databases which will be next to impossible to crack or to damage, so that the anti-viral software could block almost all viruses. However the responsibility for the attacks on particular institutions, including, state-run banks, government-owned corporations, government services providers would be strengthened, and fines would be applicable to cyber criminals. Moreover, these crimes come within the purview of the federal laws, including the laws "On state secrets" and "On banks and banking activities", etc.

In this article, the author analyzed political and legal aspects of information security and provided his viewpoint on specific political and legal actions that can be applied to assure the security in question; the author also assessed the potential improvement of confidentiality assurance methods in particular spheres of economic and state governance and political activities. The author discussed most widely spread violations in the area of informational exchange and in the field of national security. Having analyzed the present-day system of safety assurance, the author makes a conclusion that effective norms of informational legislation can serve as the basis for the issuance of bylaws needed to safeguard the subjects of political interaction. The author believes that this legal framework will help to identify potential areas for the enhancement of IT systems that can improve the safety of government authorities and subject of economic activities.

References

[1] T. Golomazova, "Sociology", Moscow, MGSU Publ., 2009.

[2] I. Bashelkhanov, "The Russia of the future needs a digital code", Russkiy Dom Publ., vol. 3, pp. 26-27, 2018.

[3] S. Mayorov, V. Kirillov, A. Pribluda, "Introduction to micro-computers", Leningrad, Mashinostroenie Publ., 1988.

[4] E. Moore, No exponential is forever: but "forever" can be delayed! International Solid-State Circuits Conference (ISSCC), 2003.

[5] O. Soldatkina, A. Malko, editor, "Using information resources of the court policy to optimize human rights policy" A roundtable discussion, Moscow, 2012, pp. 276-286.

[6] The Constitution of the Russian Federation.

[7] The Federal Law of July 21, 1993. № 5485-1 "On state secrets".

[8] Federal Law of 02.12.1990 № 395-1 "On banks and banking activities".

[9] K. Evdokimov, "Political factors of computer criminality in Russia", Yurist Publ., vol. 1, pp. 41-47, 2015.

[10] V. Melnikov, S. Kleimenov, editor, "Information security and information protection", Moscow, Akademiya Publ., pp. 51-52, 2008.

[11] V. Kopylov, "The information law", Moscow, Yurist Publ., pp. 72-73, 2002.

[12] D. Shishkin, "Youth in the virtual world", Russkiy Dom Publ., vol. 3, pp. 24-25, 2018.

[13] Federal Law of July 27, 2006 № 149-FZ "On Information, Information Technologies and Information Protection".

[14] Federal Law № 152-FZ of July 27, 2006 "On Personal Data".

[15] Federal Law of 29.07.2004 № 98-FZ "On trade secrets".

[16] M. Borodin, "The technology of a digital signature in electronic paperwork", Information Law, vol. 3, pp. 42-45, 2015.

[17] The website of the President of the Russian Federation. URL: http://kremlin.ru

[18] The Okinawa Charter of the Global Information Society of July 22, 2000", Diplomatic Bulletin, vol. 8, pp. 51-56, 2001.

[19] E. Larina, V. Obninsky, "The cyberwar of the 21st century. What Edward Snowden is silent about", Moscow, Knizhny Mir Publ., 2014. URL: https://www.litmir.me/br/?b=276514&p=1