Chapter 8

Communication Society and Security: Current Threats and Legal Maintenance

Anna A. Chebotareva, Vladimir E. Chebotarev and Alexander S. Rozanov

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.75756

Abstract

Over many centuries, human societies across the globe have established progressively closer contacts. Recently, the pace of globalization has dramatically increased. Unprecedented changes in communications, transportation, and computer technology have given the process new impetus and made the world more interdependent than ever. Information resources and structures have become a tool for achieving a strategic advantage. The authenticity, credibility, and an adequate reflection of information realities represent the key challenges for the communication society. Our research aims to analyze the possibilities of establishing a profound system for countering legalization of proceeds from crime (money laundering) and creating efficient barriers against cybercrimes, such as hacking of personal data. The sphere of security of online communication processes has become an objective element of our life, and it couldn't be ignored, especially due to further development of securing biometric personal data mechanisms.

Keywords: communication society, communication security, terrorism, offenses in the communication sphere, mechanism of remote authentication and identification, biometric personal data, money laundering, legalization of proceeds from crime

1. Introduction

The issue of balance of interests in the so-called triad "state-society-person [1, 3]" has traditionally been considered and settled by representatives of various humanitarian sciences; however, this problem is getting more and more relevant within the global communication society.

Pointing to the dialectical relationship as a characteristic of many components of the information society in the era of globalization, the authors of the research investigate the factors manifested in threats and challenges to security, the issues of reliability and objectivity of information circulated in large volumes, and the impossibility of reliable identification of online communication relations' subjects. The initiatives of the Russian parliamentarians on the formation of remote authentication and identification mechanisms, in particular, related to the creation of the national biometric platform are carefully analyzed. The resonance of the creation of national biometric platform is connected with the amendment to the law, according to which banks will be obliged to transfer biometric data of the clients to the Ministry of Internal Affairs and the Federal Security Service of the Russian Federation (FSS) for the sake of ensuring national defense, state security, law enforcement, and efficient counter-terrorism mechanisms.

Every regime of law is comprised of two essential parts: a coercive, or adjudicative, aspect and a persuasive, or educative, aspect. In the short term, a mode of governance could impose order by shear force [14]. But, over time, establishing an atmosphere of stability and continuity requires the public to understand legal authority in terms of the benefits it confers, and they must be taught habits of compliance. This combination of methods for bringing order to human life and shape to human thought forms the basis of a legal culture. In this regard, the following question seems crucially important: how to preserve the natural rights and freedoms of the individual in order to build effective communications within the society [12]? The answer is rather complicated and controversial. The process of global virtualization has made the society even more open and dependent on information data on the one hand but turned it into a highly vulnerable structure on the other hand.

The genre of our research could be characterized as a mixture of both types—an essay and an overview of the latest legislative initiatives. In this regard, the methodological basis of the research is a complex of general scientific and special legal methods of cognition. When analyzing the regularities of development of a person within a global communication society, we have been applying a dialectical approach, which has allowed us to conduct a study on the basis of two key principles—the principle of determinism and the unity of historical and logical elements of social development. Formal and logical method enabled the authors of the research to analyze the norms of information sphere's legislation, determining the content of the main concepts, and systematize the material in order to obtain generalizing conclusions.

The comparative legal method has contributed to the identification of current trends in communication society's development and to the revision of bibliography on the issue of interaction between communication technologies and society. The system analysis has made it possible to evaluate the existing approaches to legal support of communication security of a person and to relate them to objectively developing social relations. The use of a sociological method helped us to evaluate the factors influencing the behavior of a person as a subject of communication relations. The prognostic approach (in the form of modeling) was used to determine the future prospects of development of the legislation aimed at creating a system of effective legal support of a person's communication security.

http://dx.doi.org/10.5772/intechopen.75756

The methodology of our research is also based on factorial and causal analysis aimed at identifying the circumstances, which constitute threats to the individual in the communication sphere, and determining the nature of their impact on the efficiency of personal interests' implementation within the IT-space. Considering that factorial analysis as a research tool is used in various fields of knowledge, the authors propose to use this method for a comprehensive and systematic study of the nature of the communication security threats and their influence on personal data security.

2. State, technologies, and legal culture

During the early twentieth century, the nation-state had reached the height of its development and, in its various forms, had come to include within its iterations nearly the entire habitable surface of the earth. It was explicitly defined in its dimensions, protected by recognized borders, and entitled to self-defense according to defined rules of war. It was sovereign in its domestic policies, wielding exclusive authority over its people and resources. Each state was recognized as a member of the family of nations, able to enter into relations with any one of its counterparts as an equal polity.

One reason for the successful proliferation of the nation-state as a form of governance had been that the stage of technical advancement was well adapted to its limited territorial oversight. During the twentieth century, the state had been grounded in well-tested doctrines and practice, but it also fits the level of technical advance prevailing at that time. This included not only the printed book and journal but also railroad and industrial machines and, finally, radio and cinema. Combined together, these were able to create a total environment of public understanding and national purpose within a region of common language and custom.

Difficulties with the mechanism of the state began to emerge in the late twentieth century, however, because of the way further innovations in communication and transportation were being employed. Suddenly, capital could be assembled, labor concentrated, and resources marshaled, without regard to distance or topography. Sound and image could be broadcast across borders and around the world. Information of any quantity on any topic could be transmitted from any one location to any other location at any time, by any person.

For the state, these new developments—not to mention advances in warfare technology—marked a dramatic challenge not only to its functioning as a framework of authority and its foundation of national law but also to its self-sufficiency as a nation. Among the first problems to be confronted was the effective negation of its borders as a protection against unregulated communication and trade. Any former conception of the border as an absolute and defined barrier separating not only territories but also legal jurisdictions was becoming untenable.

With the great concession of the border, the next problem for national governments was the regulation of affairs that involved immigrants, visitors, and commercial agents who had entered from outside. The problem was how, on a practical level, these could be regulated or even monitored. Overseeing the affairs of its own citizens was rather easy, because both

they and their property generally existed within the region defined by national borders. But matters were less simple with those entities whose primary assets and ownership lay outside territorial limits and beyond the reach of authority.

Moreover, the new technical innovations brought instability and imbalance on an international scale as well (for instance, an outbreak of Third World protest and resistance, against what was seen as the Western exploitation of foreign and disadvantaged countries).

Complicating this reaction was another unforeseen factor: television. With the new ability to transmit sound and image, messages of discontent and revolution could be widely broadcast. Nationalist, socialist, and anti-capitalist movements in smaller countries—in the past, wholly isolated from the developed centers of power—could garner a sympathetic following around the world. Official explanations of world affairs now seemed to be undermined by the new broadcast media. The result was disruption not only in matters of foreign relations and foreign policy but also in the atmosphere of consensus necessary for quiet order and international stability. These worldwide upheavals culminated in the student rebellions of 1968.

On other hand, the positive impact of those technical innovations should not be underestimated. The arrival of the twenty-first century marked not only the advent of a new millennium but also the onset of a new age. It was termed the age of technology, of communication society, and of globalization. It was sometimes referred to as the postmodern age to distinguish it from the period of modernity that preceded it. In fact, because of remarkable advances in technology, many conventional forms of governance and rule were coming to be reconsidered.

At the beginning of the new millennium, the problems roiling the state were offset by the exhilarating impact the new technologies were having on the corporation. For that structure, electronic transmission of sound and image, voice communication, online communication systems, and computerization were unqualified benefits. The new ability to travel, to transport, and to trade opened vistas of opportunity for expansion and consolidation.

In this regard, *Andrew Feenberg*'s concept of technology (Andrew Feenberg is a proponent of a dialectical theory of technology) provides a rather clear understanding of an ambivalent nature of the interaction between the modern society and technologies: "Technological development is overdetermined by both technical and social criteria of progress, and can therefore branch in any of several different directions depending on the prevailing hegemony. … While social institutions adapt to technological development, the process of adaptation is reciprocal, and technology changes in response to the conditions in which it finds itself as much as it influences them" [6].

Technical advances greatly strengthened the ability to manage and control, extending commercial opportunities to the most remote regions of the earth. It gave great impetus to international business firms, accelerating even more the proliferation of decentralized multinational corporations. Along with these was the continuing proliferation of worldwide television broadcasting, a medium that brought enormous commercial opportunity in both entertainment and advertising.

http://dx.doi.org/10.5772/intechopen.75756

Finally, through the medium of television and other channels and networks of communication, the digital sphere could assume an educative function as well. Of course, during the human history and still now, the state has played a crucial role in this process, but with the new advances; nothing could equal the various electronic media as instruments for shaping public culture and consciousness. Unlike the old brick-and-mortar national school system, the new media could, in effect, create an artificial reality that was continuous and ubiquitous in its effects. Nothing could match its potential ability to instill habits of acceptance and compliance, a crucial necessity for an extended rule of law.

The authors of this research furthermore call to pay special attention to the issue of legal support of individuals' communication security, which is constrained by extremely complicated challenges and threats, including:

- The growth of offenses in the sphere of virtual space
- The legal issues of identification and authentication of the individual
- The imperfection of applied information and telecommunication technologies, including the possibility of technological failures, and a vulnerability of personal databases in e-government and e-justice systems
- The preservation of digital inequality
- The imperfection of a digital economy

Meanwhile, we propose to consider the communication security of a person as a state of his/her personal safety, which is determined by minimization of risks (in the form of internal and external information threats) for the individual in the conditions of global communication society, the ability to confront these challenges on the basis of a culture of communication security, as well as the formation of a state policy aimed at creation of conditions for the efficient implementation of a person's rights and freedoms in the sphere of global communications.

The interests of the individual in the online communication sphere include the implementation of constitutionally enshrined human/citizen's rights to access to information, including the use of information for the purposes of non-prohibited activities (physical, spiritual, and intellectual development), and also the protection of information that provides personal security. In this sense, we absolutely agree with *Fuchs*'s perception of the information as a dialectical process that establishes an interconnection of subjects and objects via a threefold process of cognition, communication, and cooperation [7].

It is appropriate to highlight the following legal culture mechanisms and means of providing personal communication security to be improved in the near future:

- The mechanisms aimed at the identification and authentication of individuals in the communication space, including means of biometric identification, mechanisms to ensure the protection of information, its integrity and reliability, as well as technologies of personal data protection.

- There is also a need for real adoption of interlinked organizational, scientific and technical, information and analytical, economic, and other measures to anticipate, detect, deter, prevent, and fend the information threats, as well as to eliminate the consequences of their manifestation.
- From the Russian perspective, the most urgent need of a present moment is to address the issues of high technologies development (following the example of innovative, universal blockchain platform, a quantum cryptography, etc.), the implementation of the state policies in the field of import substitution, the development of the digital economy, and the issue of a legal regulation of cryptocurrency.

The blockchain technology represents a decentralized distributed database of all confirmed transactions, whose functioning is based on cryptographic algorithms. Such technology allows:

a. To record reliable data on ownership of an asset, existed in digital format, to a certain person without the need to attract any specialized intermediary (in this case, it can be considered as a strong factor in the disintermediation of the economy)

b. To ensure that such an asset can be directly transferred to another person

In our opinion, the other relevant challenge to be resolved as soon as possible is the development of communication security's quantum cryptography system. The issues, linked to legal provision of personal communication security, are directly connected with the development of the digital currency world market (including such e-financial instruments as Bitcoin, Ethereum, etc.).

The existence of cryptocurrency transactions' anonymity without a legal regulation could be considered as an absolute risk factor, because this sort of operations is decentralized, and the absence of intermediaries leads to a quiet understandable interest of criminal organizations to gain huge profits by committing cybercrimes (including online theft and hacking). In this regard, it is necessary to officially recognize the cryptocurrency and start the legal regulation of this sphere for the purpose of ensuring communication (and also digital) security. Legal regulation of crypto-space can't be ignored; this is an objective necessity.

3. Social aspect of globalization and communication skills

Has globalization made the mankind smaller? Has the world become more intimately connected? Are the boundaries between global and local and public and personal eroding? Is this the time when nobody is perfect and no doctrine is universal? Is this the time when the abundance of choice leads to a decision paralysis? Is this the time when the world economic leaders need a facilitator to agree on a strategy for the global economy?

It has become clear that to live in a more complex, interconnected, and detailed world, the mankind needs to be equipped with tools for understanding its own behavioral patterns and

their impact on the new social dynamics. Survival in the new world means being able to navigate a gradually more unstructured and rich in detail social universe, being able to sort across a greater array of options, and possessing a deeper and more strategic understanding of self with lesser time for learning and self-discovery. What are the emerging solutions to the challenges of survival in a globalized world?

In recent years, there has been an explosion of research in psychology and social studies aimed at gaining an insight into what motivates us as species, what makes us change our ways, and what makes us happy [8, 11]. A new body of research focused on gender dynamics has provided us with a greater awareness of the needs of each gender. It explained the reasons that underlie gender-based social protocols and gave many the tools for improving their interactions with the other gender. Studies of consumer behavior have made us aware of how our brains and our feelings work when exposed to different external stimuli.

From the conversations we have to the words we choose, to the questions we ask, and to the way we think, each action or inaction speaks volumes about us. Understanding these clues and noticing the differences among individuals at an early age will make us more receptive, aware, influential, and evolved as species.

Despite the abundance of social research and the growing necessity to know the techniques for effective social interactions early in life, this valuable information has been slow in getting into school or university curriculums. Social studies continue to be confined to auxiliary subjects in business schools and catchall in university curriculums or remain in the form of bestsellers and articles in popular psychology magazines.

High schools and universities should integrate social studies and communications into a discrete social skills discipline and teach it in the way a foreign language is taught.

More scientific research of social networks is also needed. Social networks are the most vivid manifestations of globalization. They have already shown their capabilities in changing social structures, bringing people together, and creating greater prosperity in underdeveloped locales. Social networks if partnered with (and not just observed) can inform a variety of disciplines, from history and sociology to business and management. The IT industry and academia must join forces to produce new analytical data on social tools that facilitate growth and development of mankind, scale successes, and improve social climate.

4. Globalization, communication society, and Russian legal culture

Undoubtedly, the twenty-first century can be considered as the era of information accompanied by the global computerization of the modern society. The current dependence of human civilization on communication component has made it much more vulnerable in this regard. Moreover, such vulnerability is linked to the fact that our society represents itself a fundamentally open structure. The most important result of the global communication society's formation is the emergence of the so-called global communication space.

The process of society's computerization is making major changes in the social structure and the existing mechanisms for social decision-making process at all levels [17]. Globalization of social relations leads to their transformation, including new mechanisms of control and decision-making processes. Getting knowledge of ongoing social processes, discussion of trends, and forecasting possible outcomes are an important part of the goal of achieving sustainable development [7]. Nowadays the role of social consolidation of the population in the countries and regions has become even more important. Human potential in favorable conditions for the development of freethinking, informed, and responsible person could become a factor of stability, as well as successfully deal with new challenges in the form of extremism, racism, intolerance, and moral degradation [15].

Globalization of communication society is a macroscale, multifaceted, and internally contradictory process of the growth of similarity in the world communication systems (economic, political, social, and legal).

Many processes in the communication society are in a dialectical relationship and interdependence, and these relations are complex and contradictory. According to the authors of this study, the use of historical and dialectical approach (a historical context of communication and the unity of historical and logical elements of social interactions have been carefully studied by *Putnam and Pacanowsky* in 1983; for more details, see [13]) for analyzing the phenomenon of communication society is due to a number of factors [3, 4]:

1. A certain degree of inertia of the communication society and its unwillingness to fully perceive the products of scientific and technological progress (due both to objective and subjective reasons).
2. While developing and improving, the information society is not going in the direction of reducing all kinds of threats, but, on the contrary, both the number and intensity of such threats are constantly increasing [5]. The information environment is in constant development, it is moving, it is not static, and—as a result—such environment is facing obvious vulnerabilities and risks
3. The excessive amount of information is increasing exponentially; such situation leads to the fact that a person is not prepared to perceive it. As a result, the so-called internal filters have appeared: people automatically "filter" the information even before its perception, highlighting only necessary and important data for themselves.
4. The parallel coexistence of two trends: a formation of large amount of databases ("big data") with general information and—at the same time—a lack of relevant and useful information (*Ronald Day*, for instance, indicates that recently the information and communication products have been treated mainly as "reified and commoditized notion"; for more details, see [4]). The issue of reliability of the received information has become even more urgent. Another dangerous threat deserves special attention—the overload of information flows with harmful and prohibited data, as well as the misinformation.
5. The irregular and unbalanced character of information technology implementation (for comparison: in contrast to electronic workflow, paper workflow has been evolving over

the centuries). As a consequence, we are facing the mistrust to the process of implementing e-government, as well as to providing public and municipal services in an electronic form.

6. Digital technologies, used for process automation, do not have a complete form; they are in a constant process of improvement and replacement with latest upgrades. Hence, the existing solutions in the field of process automation are perceived as temporary.

7. Communication society in the context of globalization, based on cross-border concept (in this regard, *Judith Martin*'s concept of intercultural communication has a crucial meaning; see [10]), elevates the anonymity in the networks and, in turn, the identification of subjects of information relations to a level of a fundamental problem.

The central subject of communication relations [18]—a person or an identity—is subjected to serious challenges and threats; hence, the state of its security needs special attention.

The most important attributes of the personality in the modern global information world include a set of personal information, which cannot be reliably protected by technical and software means only. Personal information of the individual will be inevitably accumulated and fixed in the Internet environment (or digital space). It can be distorted and supplemented by false information that will harm the individual in terms of his or her reputation, image, breach of secrecy, etc. The person in the modern world is deprived of local protection in a macroscale environment with no national, linguistic, cultural, and even ethical boundaries.

The shift of interpersonal communication, as well as communication with society and the state into the environment, generated by the developing information and telecommunication technologies, creates conditions for a high vulnerability of the personality in the global world.

The interests of a person in the information sphere are to meet all his/her possible needs—to ensure the right to access to information; the possibility of citizen's participation in lawmaking activities, including through the development of electronic democracy mechanisms; the possibility of obtaining state and municipal services in electronic form, as well as the implementation of the right to protection through electronic justice mechanisms; etc.

The global information society appears as a platform for the development of both positive and deterrent factors: the first one contributes to the realization of the whole spectrum of interests of the individual; the last one hinders the development of the information society itself (as a whole).

The global, cross-border nature of information and telecommunication technologies leads to the immensity of offenses in the information sphere; this trend, in turn, leads to a significant violation of the rights and interests of the individual. The significance of risks and threats can cause serious damage in the implementation of personal interests in the global communication society. This fact can be proved by:

- The identification issues
- The possibility of falsifying the results of online voting ("e-voting" [14])
- The possibilities of technological failures in the process of development of electronic parliament elements and electronic democracy mechanisms [9]

- The possibility of unreliability of databases
- The insecurity of confidential information and personal data in the provision of public and municipal services in an electronic form
- The potential danger of unfair use of personal data in the process of development of electronic justice mechanisms
- The problem of distribution of illegal and harmful content, directly threatening human health, and disorienting the person
- The problem of distribution of defamatory materials by electronic media [18]
- The possibility of theft of information, used in the Internet banking systems [16]
- The possibility of loss of data as a result of malicious attacks while working on the Internet (hacking)

The uniqueness of the virtual environment forces the subjects of information relations to adapt, looking for ways and opportunities for existing in "real-life [3]" conditions. At the moment, for instance, we are facing the processes of transferring credit institutions' activities into the virtual environment and the development of digital financial services. The Russian State Duma (the lower house of the Russian Parliament) has been consistently implementing since April 2017 an initiative to create a legal framework for the use of remote authentication and identification mechanism, through which credit institutions will be able to open accounts to individuals (natural persons) via the Internet. The Project Law "On Amendments to the Federal Law" "About counteraction of legalization (washing) of income gained in the criminal way and to terrorism financing" also regulates the procedure for collection and transfer of personal data (including biometrics) into a single system—a Unified System of Identification and Authentication (USIA). USIA is a system created and developed by the Russian Ministry of Communications within the e-government infrastructure in order to streamline and centralize the processes of registration, identification, authentication, and authorization of users.

According to the plan of the Russian parliamentarians, a citizen will need to come to the bank once in order to provide personal data; soon after that, he or she will be able to open accounts without personal presence. At the same time, the main condition to be satisfied by the remote identification of the customer of the credit institution is the absence of his/her involvement in the legalization and laundering of proceeds from crime, as well as in extremist or terrorist activities. And it is not just about personal data. This initiative supports the procedure of interactive remote authentication and identification of the client of credit institution by using citizen's biometrics.

The document provides for the obligation of banks, included in the special list established by the Central Bank of the Russian Federation, on behalf and with the consent of the client (natural person) in order to conduct further remote identification, including other credit institutions, to collect and transfer the following data into the USIA:

- Last name and first name of a person, person's patronymic (if the other does not follow from the law or national custom), a citizenship, a date of birth, an identity document number, a

migration card number, the data of a document confirming the foreign citizen or the person without citizenship on stay (residence) in the Russian Federation, the address of residence (registration) or place of stay, taxpayer identification number (if any), an insurance number of individual personal account, and the number of mobile telephone communications subscriber (mobile phone number).

- Information on client's biometric personal data.
- Information on the client's consent to the processing of his/her personal data, including the unified identification and authentication system and information technology elements that ensure the collection, processing, storage, and provision of biometric personal data.

A range of practical important issues has been revealed during the adoption stage of this draft law (a bill). First of all, the agenda includes the establishment of the system of protection of customers' biometrics, the cost of its implementation, as well as the mechanism or the process of customer's face and voice identification.

At the final stage of drafting of this bill, the State Duma of the Russian Federation had adopted the law on the creation of a mechanism for interactive remote authentication and identification of the customer of the credit institution—a law "On amendments to certain legislative acts of the Russian Federation [3]." This change in the Russian legislation will allow banks to open accounts to individuals (natural persons) without their personal presence, only with the use of biometric passports and data, uploaded to the "Public Services" web portal.

In turn, the law on combating legalization (laundering) of proceeds from crime is supplemented by provisions according to which the banks, included in the list of the Central Bank, on behalf and with the consent of the customer (natural person), can operate with his/her personal data, uploaded into the USIA database.

In general, the system of remote identification of credit institutions' customers (natural persons) is proposed to be based on the processing and use of biometric personal data, since such identification has the highest degree of reliability in the digital space.

The pilot project of the mechanism of implementation of the law is expected to be tested on a limited number of bank operations.

The new law has caused a wide resonance; its reason has appeared during the second reading of the bill. This is an amendment according to which banks will be obliged to transfer biometric data of clients to the Russian Ministry of Internal Affairs and the Federal Security Service (FSS) for the sake of national defense, state security, law enforcement, and counter-terrorism. It is adopted that the order of data transfer will be established by the government. At the same time, it is not indicated that the consent of the bank's client is necessary.

The alleged violation of privacy (Article 23 of the Russian Constitution) and the possibility of issuing personal data to the Ministry of Internal Affairs and FSS have evoked a protest mood. We would like to remind that according to Article 23 of the Constitution of the Russian Federation, everyone has the right to inviolability of private life, a personal and family secret, and protection of the honor and reputation.

There is a certain contradiction of the analyzed norms to the Federal Law "On personal data," which directly prohibits the processing of personal data for purposes not specified in their collection. According to Dmitry Yanin, the President of the International Confederation of Consumer Societies, "… getting the biometric data in exchange for online access to services is an unequal fee, there is a high probability of leakage… In fact, you can consider that biometrics will soon be available to all [15]." In Russia, the problem of availability of financial services is not acute; it is better to go to the bank and not share data—it is difficult to predict who will use them and in what way.

As for the problematic issue of creating a full-fledged protection of biometric data of banks' clients, the law provides that for the provision of biometric personal data of an individual through the channels of information transfer for the purpose of his/her identification without personal presence via the Internet, the encryption (cryptographic) means should be used to ensure the security of transmitted data from security threats, relevant in the processing of biometric personal data [5, 15].

The envisaged obtaining the consent of a citizen of the Russian Federation to the processing of personal data and biometric personal data for the implementation of his/her identification may be signed by his/her simple electronic signature, the key of which is obtained in accordance with the rules for the use of a simple electronic signature when applying for state (public) and municipal services in electronic form, established by the Government of the Russian Federation.

The digital identification operator for the banking sector will be "Rostelecom" (Russian state universal telecom operator), which will create the so-called National Biometric Platform (NBP). At the same time, it is planned to use NBP in medicine, education, and retail, in multifunctional and certification centers, and in departments of the Ministry of Internal Affairs.

NBP is supposed to represent a set of specialized information and technological elements that enable the collection, processing, storage, allocation, and compliance of biometric data.

This platform will be located in the secure cloud infrastructure of "Rostelecom," which will be accessed by banks through special communication channels of the system of interdepartmental electronic interaction (SIEI).

In connection with the latest initiatives of the Russian parliamentarians, a number of "painful" points should be noted. The creation of remote authentication and identification mechanisms is aimed, according to the government's plan, at ensuring security and countering the financing of terrorism and the legalization (laundering) of proceeds from crime. It is on one side of the scale. On the other side, we are witnessing the opportunities for violation of our privacy, the danger of incomplete protection of biometric data of bank customers, as well as the threat of its loss, theft, and free access. The obligation, imposed on banks to transmit client biometric data to the Russian Ministry of Internal Affairs and the Federal Security Service for the sake of national defense, state security, law enforcement, and counter-terrorism, may open up wide opportunities for the abuse of such data.

There is a danger to repeat our previous mistakes. Moreover, when studying the peculiarities of crimes in the banking sector, committed using high technology, on the example of data in

http://dx.doi.org/10.5772/intechopen.75756

June 2016, we have already noted that Russia ranks second in the world rating in the number of information leaks in the financial sector. At the same time, in 73 percent of cases, customers' personal data had been lost or stolen from the Russian banks. As a result, more than 22.5 million personal data records had been leaked to the Internet.

Russian banking system has more than enough problems without the system of remote authentication and identification, which is created and planned to be implemented. Thus, specialists-practitioners in the field of Internet banking and remote banking are right, stating that "the rapid development of Internet technologies does not allow us to predict all the strategic risks… [1, 15]." For instance, Professor Savenkov notes that "many banking institutions underestimate the threat of hacker attacks, without building an adequate system of information security, and thereby create conditions for large-scale theft of funds [15]."

The result is the fact of toughening criminal liability for the crimes, committed in the mass use of payment services in the context of the increased risk of illegal access, destruction, modification, blocking, copying, provision, and dissemination of information, as well as other illegal actions promoted by the development of high technologies.

Speaking about the so-called sensitive information, it should be noted that the attention to the components of this concept—personal information, private life information, as well as personal data, including biometrics—is drawn from the entire world community.

Recently, the National Association of State Chief Information Officers (NASCIO) has published an action plan for a reasonable investment in cybersecurity entitled "Better Data Security Through Classification: A Game Plan for Smart Cybersecurity Investments [2, 3, 5]."

This plan attempts to classify the data by gravity consequences of unauthorized access to them. At the same time, the document explains why the risk-based approach to cybersecurity is the best option for protecting the data of state organizations. Using this approach, the efficiency of operational management increases, the evaluation of the value of information assets becomes more accurate, the ability of hackers to attack these assets is reduced, and the decision-making process is improved.

Data security is always critical for government agencies, so government IT directors have identified data management and data analytics (including data architecture, big data, predictive analytics, etc.) as a priority for 2017.

The classification is defined as "the process of identifying information that needs to be protected from unauthorized access and misuse [3, 5]." Each federal agency should be the competent classification authority for the data and information it collects or uses for the performance of its tasks.

The following classification is proposed:

1. Critical data—the data of critical importance (it is impossible to carry out the most important state functions without them, e.g., the cadastral records or a register of voters)
2. Sensitive information—the information, if it is disclosed or stolen, which may cause damage to a citizen (e.g., tax data or bank statements)

3. Medical data—the information, which includes a significant amount of personal health information that can be used to discriminate a citizen if it falls into the public domain or into the hands of a hacker
4. The information used to identify people (personally identifiable information or PII)—basically it is data collected by financial and similar institutions

It is necessary to emphasize that the possible compromise of PII can lead to identity theft with a variety of consequences, including primarily the theft of money from the accounts of the citizen.

Other important information that does not fit into these categories, but also requires protection, may be available to government agencies.

The data classification, developed by NASCIO, should be taken into serious consideration. The criterion, laid down in its basis (severity of consequences of unauthorized access to data), contributes to a more accurate assessment of risks (challenges and threats) in the information sphere. And today such assessment is very actual and is capable to minimize committed offenses in the conditions of global and transboundary character of rapidly developing information and telecommunication technologies.

5. Conclusions

In today's society, it is impossible to exist without social networks and different Internet technologies. Currently every person, connected to a computer, has to register in at least one social network. Many people do not care about the security of their personal data. But almost any site requires us to enter basic personal information, such as names and the date of birth. Most visitors of the Internet have the same password on all sites, which is a plus for hackers.

Personal data security is a state of personal data security characterized by the ability of users, technical means, and online communication technologies to ensure confidentiality, integrity, and availability of personal data during their processing in personal data communication systems.

Communication security is becoming a key factor in the provision of electronic services. Modern communication services are distinguished by the use of a large amount of sensitive information that needs protection (personal data, payment information, keys, and secrets).

The possibility of creating a National Biometric Platform could provide remote authentication, based on the biometric features of users in any remote service channels: mobile applications, web clients, or points of contact. Such a platform will become not only more reliable and convenient than password or SMS protection; it will also allow to operate a mechanism of remote access to public services. Thus, it could become a tool for improving the efficiency of interaction between the state, business elites, and society.

Among the possible areas of application of NBP are e-government (public services), telemedicine, distance education, e-commerce (including control of remote purchases of medicines),

and financial and legal sectors of the economy in terms of transaction confirmation. It is also possible to use the platform for biometric access control to important infrastructure facilities, such as sports stadiums.

Author details

Anna A. Chebotareva, Vladimir E. Chebotarev and Alexander S. Rozanov*

*Address all correspondence to: rozanov-88@list.ru

Russian University of Transport (The Institute of Law), Moscow, Russian Federation

References

[1] Abbate J. Inventing the Internet. Cambridge: MIT Press; 2000

[2] Bradberry T, Greaves J. Emotional Intelligence 2.0. San Diego: Talent Smart; 2009

[3] Chebotareva A. Cybercrime in the banking sector: The main directions of the criminal policy of the Russian Federation. The Criminological Magazine of the Baikal State University of Economics and Law. 2014:140-144

[4] Day RE. The Modern Invention of Information: Discourse, History, and Power. Carbondale: Southern Illinois University Press; 2001

[5] Tardy T. European Security in a Global Context. Internal and External Dynamics. Routledge; 2010

[6] Feenberg A. Transforming Technology: A Critical Theory Revisited. Oxford: Oxford University Press; 2002

[7] Fuchs C. Information and communication technologies & society: A contribution to the critique of the political economy of the internet. European Journal of Communication. 2009;**24**(1):69-87

[8] Gumucio DA. Making Waves: Stories of Participatory Communication for Social Change. New York: Rockefeller Foundation Report; 2001

[9] Grossman LK. The Electronic Republic: Reshaping Democracy in the Information Age. New York: Viking; 1995

[10] Martin JN. Intercultural Communication in Contexts. New York: McGraw-Hill; 2010

[11] Medina J. Brain Rules. Seattle: Pear Press; 2008

[12] Minchenko T. The dynamic model of freedom of conscience in the modern world. European Social Science Journal. 2014:533-537

[13] Putnam L, Pacanowsky M. Communication and Organizations, an Interpretive Approach. Newbury Park: Sage Publications; 1983. 303p

[14] Rhodes R. Understanding Governance. Policy Networks, Governance, Reflexivity and Accountability. Buckingham; 1997

[15] Savenkov A. Criminal policy and the stability of the financial and credit system. Journal of Russian Law. 2016:78-91

[16] Sychev A, Revenkov P, Dudka A. E-Banking Security. Moscow: RK-Laboratory Image; 2016. 212p

[17] Teisman GR. Models for Research into Decision-Making Processes: On Phases, Streams and Decision-Making Rounds. Public Administration; 2000

[18] Acuña BP, editor. The Evolution of Media Communication. InTech; 2017. DOI: 10.5772/6516