global-e

Information Risk: A Proposed Biometric Data Law in Russia

August 22, 2019 | Volume 12 | Issue 35
Alexander Rozanov
Michael Smirnov
Mariya Krotovskaya
Alexandra Baranova
Aleksandra V. Khramova

Without a doubt, the twenty-first century can be considered as the era of information accompanied by the worldwide computerization of society. But human civilization's present dependence on communication technology has made individuals much more vulnerable due to the fact that modern societies represent themselves as fundamentally open and transparent structures. Although constantly developing and improving, information societies struggle to reduce all kinds of threats at a time when the number and intensity of such threats are constantly increasing (Tardy 2010). The information environment is not static, and as a result it faces obvious vulnerabilities and risks. Therefore numerous processes in global communication society are embedded in dialectical relationships of interdependence, relations that are complex and often contradictory.

Today's world witnesses the parallel co-existence of two trends: the formation of large numbers of databases ("big data") containing specific, discrete information, and at the same time, a torrent of irrelevant and doubtfully useful information.[1] The issue of reliability of received information has become even more urgent, while at the same time there is an overload of information flows involving harmful and prohibited data. The irregular, unbalanced, and rapidly changing character of information technology implementation has a further consequence—the generation of mistrust in the process of implementing e-government infrastructure and providing public and municipal services in electronic form.

Communication society in the context of globalization, based on a cross-border, "intercultural" concept[2] that results in the elevating anonymity in networks, in turn raises a fundamental problem regarding the identification and social construction of

subjects. That is, the central subject of communication relations (Peña Acuña 2017)—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 alone. Personal information of the individual will inevitably be accumulated and fixed in the internet environment (or digital space). It can be distorted and supplemented by false information that would harm the individual in terms of her or his reputation, image, breach of secrecy, and so forth. The person in the modern world is deprived of local protection in macro-scale environment with few and often contradictory national, linguistic, cultural, and even ethical boundaries.

Ideally, the interests of a person in the information sphere are to meet all his/her possible needs: to ensure the right to access information, to participate as a citizen in law-making activities through developments such as electronic democracy mechanisms, to obtain state and municipal services in electronic form, to secure protection through electronic justice mechanisms (e.g., an electronic system of appeal against court decisions, legal advice online through smartphone apps, electronic feedback forms, etc.), among others.

A Case Example from Russia

As one example, the development of digital financial services has transferred credit institutions' activities into the virtual environment. Since April 2017 the Russian State Duma (the Lower House of the Russian Parliament) has been advancing an initiative to create a legal framework for the use of a remote authentication and identification mechanism through which credit institutions will be able to open accounts to individuals (natural persons) via the Internet. The Draft Law “On amendments to the Federal Law about counteracting legalization (washing) of income gained in criminal conduct and about 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 would need to come

to the bank just once in order to provide personal data. Soon after that he or she will be able to open accounts without personal presence. The main condition to be satisfied by remote identification of the customer is verification that they are not involved in the legalization and laundering of proceeds from crime, including those derived from extremist or terrorist activities. And it's not just about personal data. This initiative supports interactive remote authentication and identification by using citizen's biometrics. The pilot project of the mechanism for the law’s implementation is expected to be tested on a limited number of bank operations.

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 alone.

A range of important practical issues was revealed during the adoption stage of this draft law. First of all, the legislation’s agenda includes the establishment of 1) a mechanism or process for face and voice identification, 2) a system for protecting customer biometrics, and 3) the cost of the law’s implementation. The new law has generated widespread reaction that began during the second reading of the bill, involving an amendment according to which banks would 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. The order to initiate this data transfer would be established by the government, yet the draft legislation does not indicate that the consent of banks’ clients is required for this transfer.

Russian Federal Security Service building, Moscow. (Image source: Wikimedia)

The alleged violation of privacy and the possibility of issuing personal data to the Ministry of Internal Affairs and FSS have evoked a mood of protest. According to Article 23 of the Constitution of the Russian Federation, everyone has an inalienable

right to a private life, to protection of personal and family secrecy, and protection of their honor and reputation.

There is a certain contradiction in the norms of 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 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.” (Savenkov 2016)

As for the problematic issue of creating full-fledged protection of individual bank clients’ biometric data, the law provides that encryption (cryptographic) technologies should be used for such information transfers via the Internet. In this way identification without personal presence is expected to ensure protection of transmitted data from security threats (Tardy 2010, Savenkov 2016).

The alleged violation of privacy and the possibility of issuing personal data to the Ministry of Internal Affairs and FSS have evoked a mood of protest.

The digital identification operator for the banking sector would be Rostelecom (Russian state universal telecom operator), which will create the so-called National Biometric Platform (NBP). At the same time, NBP is planned for use in medical, educational, and retail settings, 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 would be located in the secure cloud infrastructure of “Rostelecom,” which would be accessed by banks through special communication channels of the System of Interdepartmental Electronic Interaction (SIEI).

Problems with the Proposed Data Law

In connection with these 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 by countering the financing of terrorism and the legalization (laundering) of

proceeds from crime. This represents one side of the scale. On the other, we are witnessing the creation of opportunities for violation of our privacy, the danger of incomplete protection of the 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 may open up many opportunities for the abuse of such data.

There is a danger of repeating previous mistakes. For example, when studying the peculiarities of crimes in the banking sector committed using high technology (based on data from June 2016), we noted that Russia ranks second in the world in the number of information leaks in this sector. In 73 percent of cases, customers' personal data had been lost or stolen from Russian banks. As a result, more than 22.5 million personal data records have been leaked to the Internet.

The Russian banking system has more than enough problems without implementing the planned system of remote authentication and identification. Specialist-practitioners in the field of Internet banking and remote banking are right when they state that “the rapid development of Internet technologies does not allow us to predict all the strategic risks...” Considering that personal data security depends on the ability of users, technical systems, and online communication technologies to ensure confidentiality, integrity, and availability of personal data during their processing in personal data communication systems, the switch to a biometric data collection system as currently proposed seems a risk not worth taking. Yet the proposed Russian law is characteristic of worldwide trends toward digitalization of, and vulnerability of, identity in the 21st century.

Notes

1. Ronald Day (2001), for instance, indicates that recently the information and communication products have been treated mainly as a “reified and commoditized notion.”

2. By this we mean the ethnic and cultural matrix of business communications, ethnic labels, jokes and prejudices, cultural and linguistic differences, compatibility of interests and values, acuteness of ethnic differences, prehistory of cultural relations, intercultural contacts, and potential for interaction. In this regard, Judith Martin's concept of intercultural communication has a crucial meaning; see Martin 2010.

3. 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.” See Savenkov 2016. See also Abbate 2000.

References

Abbate, J. *Inventing the Internet*. Cambridge: MIT Press, 2000.

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.

Day, Ronald E. *The modern invention of information: Discourse, history, and power*. Carbondale, IL: Southern Illinois University Press, 2001.

Tardy, T. (Ed.) *European Security in a Global Context. Internal and External Dynamics*. Routledge, 2010.

Fuchs, C. “Information and communication technologies & society: A contribution to the critique of the political economy of the Internet.” *European Journal of Communication* 24 (1) 2009; 69-87.

Martin, Judith N. *Intercultural communication in contexts*. New York: McGraw-Hill, 2010.

Savenkov, A. “Criminal policy and the stability of the financial and credit system.” *Journal of Russian law*. 2016; 78-91.

Sychev A., Revenkov P., Dudka A. *E-banking Security*. Moscow: RK-Laboratory Image, 2016.

Teisman, G.R. *Models For Research into Decision-Making Processes: On Phases, Streams and Decision-Making Rounds*. Public Administration, 2000.

Peña Acuña, B. (Ed.) *The Evolution of Media Communication*. InTech, 2017; DOI: 10.5772/6516.

See Also

Gumucio Dagrón A. "Making Waves: Stories of Participatory Communication for Social Change." New York: Rockefeller Foundation Report, 2001.

Grossman L.K. *The Electronic Republic: Reshaping Democracy in the Information Age* . New York: Viking, 1995.

Medina J. *Brain Rules*. Seattle: Pear Press, 2008.

Minchenko T. “The dynamic model of freedom of conscience in the modern world.” *European Social Science Journal* 2014, pp. 533-537.

Putnam L., Pacanowsky M. *Communication and organizations, an interpretive approach*. Sage Publications, 1983, p. 303.

Rhodes R. *Understanding Governance. Policy Networks, Governance, Reflexivity and Accountability*. Buckingham: Open University, 1997.

Rogers E. *Communication and Development: The Passing of the Dominant Paradigm. Communication and Development: Critical Perspectives*. London: Sage, 1976, pp. 121-148.

Rogers E. *New Perspectives on Communication and Development: Overview*. Communication Research. London: Sage, 1976, pp. 99-107.

Rogers E, Kincaid D. *Communication Networks: Toward a New Paradigm for Research*. New York: Free Press, 1981.

Sychev A, Revenkov P, Dudka A. *E-banking Security*. Moscow: RK-Laboratory Image, 2016, p. 212.

Tags

technology

security

Alexander Rozanov, Russian Academy of National Economy and Public Administration, CREON Group expert, Moscow, Russian Federation.

Michael Smirnov is a practicing lawyer and member, Russian Academy of National Economy and Public Administration, Moscow, Russian Federation.

Mariya Krotovskaya is a member, Russian Academy of National Economy and Public Administration, Moscow, Russian Federation.

Alexandra Baranova is a member, Russian Academy of National Economy and Public Administration, Moscow, Russian Federation.

Aleksandra V. Khramova is a PhD student in the Department of Political Science at Lomonosov Moscow State University.

View PDF