Privacy of genetic data: issues with legislation and law enforcement in the Russian Federation

Semiakina Anna[1]
Law Institute, Tomsk State University

Summary. This article aims to evaluate the "gray areas" in Russian legislation regulating the activities of medical organizations for the processing of genetic data as personal data. The analysis includes the relevance of the topic for the economy, science, and law in Russia, and current legislation from the perspective of gaps and enforcement issues. The paper also provides brief recommendations for improving legal regulation in the field of genetic data processing and associated risks.

Genetic research in the Russian Federation is gaining its place in the market for high-tech medical services. So, services for assessing the state of health and risks of hereditary diseases, assisting in the planning of a child, determining dietary features, and evaluat-

[1] Email: siemiakina.anna@mail.ru

ing medications effects are becoming more and more popular and accessible. Genetic clinics provide genetic counselling via Skype, courier picking up genetic material, and receiving results remotely through clients' accounts on clinics' servers. Pharmaceutical companies are showing interest in creating integrated biomedical databases.

In 2018, genetic research expanded markedly in Russia. The Russian company R-Pharm announced plans to build centers for genetic research in conjunction with the Human Longevity Inc. in the US. The Japanese pharmaceutical company Takeda and the Institute of Cytology and Genetics of the Siberian Branch of the Russian Academy of Sciences announced the completion of a joint project - an integrated database that accumulates research data, pathology mechanisms, and treatment results that the company plans to use to develop new drugs. Also, in 2018, the Skolkovo Institute of Science and Technology and the Medical Genetic Research Center signed a memorandum on the CoBrain Analytics project to create a common medical information database based on an analysis of the patient's genetic data.

In addition, there is also interest by the State in carrying out a genetic identification of the population, the development of gene pool screening technology. In 2019, the Government of the Russian Federation approved the Federal Scientific and Technical Program for the Development of Genetic Technologies for 2019–2027. The Russian Government's task of accumulating personal information about citizens is becoming technically feasible following the switching to digital health records – the creation of the Unified State Information System in Healthcare (EGISZ).

In 2017, Federal Law No. 187 "On the Security of Critical Information Infrastructure of the Russian Federation" was adopted, aimed at ensuring the information security of economic entities. In addition, over the past 6 years, by-laws of different authorities have been adopted: decrees of the Government of the Russian Federation (dated July 6, 2015 No. 676, dated February 8, 2018 No.

127, dated May 5, 2018 No. 555, and April 12, 2018 No. 447); Order of the Ministry of Health of Russia dated June 17, 2019 No. 911n; Orders of the Federal Service for Technical and Export Control - hereinafter referred to as FSTEC (dated February 11, 2013 No. 17, dated February 18, 2013 No. 21, dated March 14, 2014 No. 31, dated December 25, 2017 No. 239).

This updating of legislation confirmed that the previously adopted laws (the Federal Law “On the protection of citizens’ health”, “On personal data”, “On information, information technology and the protection of information”) lagged behind scientific and technological progress. In particular, the duty of the owners of critical information infrastructure (CII) is to notify the FSTEC about cyberattacks. The FSTEC clarified the requirements for information protection at CII objects, as well as about the list of CII objects to be categorized. A list of information provided to the State system for detecting, preventing, and eliminating the consequences of computer attacks has been compiled, and a procedure for exchanging information with the subject of CII has been determined. The requirements of the Ministry of Health, which come into force on January 1, 2020, tighten the norms 17 and 21 of the FSTEC Orders: the requirements for the protection of information contained in information systems and the hardware and software of these systems are defined; established the mandatory requirements for the certification of the information security tools in medical organizations. The servers of such information systems should locate on the territory of the Russian Federation.

Despite significant changes in the field of processing personal data and ensuring information security, there is still a lack of guidelines, and an abundance of documents, often duplicating each other. Prior to the adoption of these acts, medical organizations in the Russian Federation were entitled to choose at their own risk and the allocated funding information security technologies that provide: separate storage of personal information about the patient and genetic data; use of servers and communication channels pro-

tected from external threats; authorized access to processed and stored data; data encryption and anonymization; copy protection; creating backup copies of data, etc.

In this regard, it would be possible to assume a sufficient level of protection of the personal data in the Russian Federation if it were not for serious data breaches. For example, two cases of mass leakage were reported in the media in 2019 in the Moscow Region and Lipetsk. So, according to media reports, in the first case, the file server of the ambulance service of the Moscow Region was accessible from the Internet, and there was no user authorization system. An outdated version of the file-sharing protocol was being used. The connected guest could edit and delete files. As a result of such attacks, the number of victims is estimated to be thousands, and in the future, it can be millions. Breach threats are serious, including because of the lack of appropriate sanctions in the Federal Law "On Information…" and the lack of differentiation of liability (controller, data processor).

Along with the existing lacunae and inconsistency of the legislation, it is also necessary to note the excessive discretion of the medical organization in determining rights, and the diffusion of liability among themselves and patients in practice. Representatives of relevant ministries in the Russian Federation noted the vagueness of the wording in the form of informed consent of a patient (access to primary documentation vs. transfer of anonymized data).[2] There are attempts to shift the liability from the medical organization to the sponsor of the genetic research or to exempt the doctor-researcher from the obligation to keep medical privacy, contrary to the provisions of federal law. Often, medical organizations

[2] Elena Volskaya. *Protection of personal data of patients participating in scientific and clinical research. Report at a meeting of the Council of public organizations for the protection of patients' rights at the Federal Service for Supervision of Healthcare* (September 18, 2018), http://www.roszdravnadzor.ru/i/upload/images/2018/9/18/1537283104.03682-1-1443.pdf (accessed Dec. 17, 2019).

shift the liability and risks of maintaining privacy to the patient and expand the list of people who can access the patient's primary medical documentation.

Finally, the current legislation of the Russian Federation does not consider the peculiarities of genetic data as object of high commercial value to various economic entities, as well as allowing the identification of other persons. Fixing the status of genetic data as personal and biometric, proposed by the bill of the Government of the Russian Federation, is not enough.[3] The current federal laws do not specifically regulate the issues of obtaining and processing DNA information, informing a person about the progress and results of genetic research, disclosing and protecting the privacy of the data received. The law does not define the right to withdraw informed consent and the procedure for cross-border transfer of genetic data. There is no regulation on permissible disclosure of medical information in special cases (informing relatives, representatives of the patient). The legislator has not resolved the question of the permissibility of a person's open consent to the widespread use of their genetic material, not only for scientific purposes that already provided but also for purposes that may arise in the dynamics of the research process. More detailed regulation in the Russian Federation may need to address the issues of individuals' rights in cases where personal data are processed by data processors. So, it is possible to resolve the issue by sharing the profit of genetic research with individuals who provided their genetic data.

The Russian legislator also needs to take into account international regulatory experience and, in particular, the EU General Data Protection Regulation (GDPR). The Regulation, although providing insufficient protection for the individual[4], provides some

[3] Bill № 744029-7 On amendments to Article 11 of the Federal Law "On Personal Data" regarding the processing of biometric personal data (2019)

[4] Selita, F. 2019. Genetic Data Misuse: Risk to Fundamental Human Rights in Developed Economies. *Legal Issues Journal*, 7(1). DOI: doi.org/10.6084/m9.figshare.11423724

new expanded rights and obligations for people who provide data, that have no analogues in Russian legislation. For example, the regulation defines the duty to notify the operator not only the authorities, but also the subject - the carrier of personal data about the case of leakage of such data. The right to data portability between operators, the right to restrict processing, and the right to notify a subject when changing or destroying his personal data provided. The GDPR also determines significant fines for non-compliance with European legislation, independent supervisory authority, and the right of a person to protect his rights effectively.

Overall, two conclusions can be made. First: the use of genetic data in the Russian Federation require special regulation that provides, on the one hand, effective protection of the rights of individuals, and on the other hand, does not create additional restrictions on the conducting of genetic research, including the joint work with foreign organizations. The second conclusion relates to the provisions of Part 2 of Art. 11 of the Federal Law “On Personal Data”, expanding the list of cases of processing biometric personal data without the consent of a person for the purposes of the administration of justice and the enforcement of judicial acts, for state defense and countering terrorism, transport security, combating corruption, operational-search activity, public service, and migration. Together with the general genetic identification of the population in the Russian Federation, this regulation will entail changes in the concept of privacy in the Russian Federation.[5] However, is privacy possible in cases where biobanks are State-controlled? Would such practices of the State contradict the provisions of international acts in the field of protection of human rights? In order to answer these questions more public discussion is needed in the Russian Federation.

[5] Ellen W. Clayton, Barbara J Evans, James W Hazel, Mark A Rotstein, *The law of genetic privacy: applications, implications, and limitations*, Journal of Law and the Biosciences Vol 6 Issue 1 (2019).