International Journal of Law in Changing World

Volume 1 Issue 2 (2022) ISSN 2764-6068

Research article
Journal Link: https://ijlcw.emnuvens.com.br/revista
DOI: https://doi.org/10.54934/ijlcw.v1i2.29

PATIENTS' PERSONAL DATA, INCLUDING BIOMETRICS, AS OBJECTS OF CRIMINAL LAW PROTECTION

Albina Shutova
Department of Criminal Law and Procedure,
Kazan Innovative University named after V.G. Timiryasov, Kazan, Russian Federation

Article Information:

Received
October 17, 2022
Approved
October 18, 2022
Accepted
October 29, 2022
Published
December 29, 2022

Keywords:

personal data,
crimes, biometric
personal data,
criminal law,
medical secrecy

ABSTRACT

Objective. The article is devoted to the issues of criminal law regulation of personal data of patients constituting a medical secret. The purpose of the study is to assess the level of legal regulation of social relations against which criminal encroachments are committed in the processing of personal data, as well as the improvement of Russian criminal legislation in this area. **Methods.** A literature review was conducted of studies published in the Dimensions and Elibrary databases. We have selected 16 papers published in full text, online and free of charge in 2010-2020. **Findings.** The institution of personal data, including biometric data, is wider than the institution of medical secrecy and includes a wider range of information about the patient. The institution of personal data is universal, as it is aimed at regulating public relations in various spheres of public life, and the institution of medical secrecy is only in the healthcare system.

FOR CITATION:

Shutova, A. (2022). Patients' Personal Data, Including Biometrics, as Objects of Criminal Law Protection. International Journal of Law in Changing World, 1 (2), 46-59. DOI: https://doi.org/10.54934/ijlcw.v1i2.29

1. INTRODUCTION

Contemporary life necessitates rendering high-quality medical services to the population, which inevitably leads to improvement and increased attention to high-technology medical aid. Undoubtedly, the observed scientific and technical progress actualized the need to integrate medical technologies into the legal framework. The Concept of developing regulation of relations in the sphere of artificial intelligence technologies and robotics up to 2024, adopted by the Decree of the Russian Government of 19 August 2020 no. 2129-r, pays significant attention to such area of improvement as *regulation of applying the artificial intelligence technologies and robotics to the sphere of healthcare*.

Taking into account the prospects of further active introduction of robotized medicine, we would like to highlight the area which is, in our opinion, not yet sufficiently regulated and needs further improvement. When rendering medical aid, including surgical, medical robots interact with humans and may collect and store a large amount of information about the patients (about their health, fact of application, diagnosis, information about treatment, etc.) and their biometric data. In this regard, the issues of informational security of the patients' personal data and the state of criminal-legal regulation of public relations in this sphere are topical. This issue is also relevant in the aspect of transition of medical institutions to electronic document flow, which also contains a large amount of patients' data. In general, the global community pays great attention to both personal data protection and legislative changes in respect of confidentiality (Lopes, Guarda, Oliveira, 2020).

2. PATIENT PERSONAL DATA AND CRIMINAL LAW

2.1 Personal data: concept

With the development of digital technologies and improvement of medical services, the volume of patients' biometric data will increase. Most of the information previously kept on paper is now digitally transmitted, which creates new digital challenges and threats in relation to security and confidence, particularly, in relation to protecting personal data in the society which becomes more and more digital (Mitchell, Kan, 2019).

https://doi.org/ 10.54934/ijlcw.v1i2.29

We should agree with A. A. Mokhov, who believes that biobanks are created in Russia, thus the risks increase of illegal acquisition of information which characterizes the biological essence of the relevant persons (Mokhov, 2021).

Assumingly, the patient's data acquired by wrongdoers via illegal access may threaten citizens' confidentiality. Actions of a surgeon, tactile feedback, and video recordings of a medical robot may contain personal information, including naked parts of the body of a patient. This opinion is shared by E. E. Istratova and A. A. Molchanov, who emphasize that the most critical aspects of medical robots are the aspects of safety (in a broader sense – both physical and informational) and (Istratova, Molchanov, 2015). We should agree with foreign authors in that medical confidentiality is a subject for disputes, as it is necessary to protect a patient's privacy and, at the same time, bear responsibility for preserving other people's health (Raimundo, Grando, Machado, Oliveira, Cabar, 2022). The regime of personal data protection is of particular concern due to their vulnerability, probable illegal actions, discrimination, and unethical illegal use (Alrefaei, A.F., Hawsawi, Y.M., Almaleki, D. et al., 2022). At the same time, the polls on personalized medicine held in Pennsylvania (USA) and Bavaria (Germany) showed that most of the respondents were concerned about misuse of genetic data (Kichko, K., Marschall, P.&Flessa, S., 2016).

While processing personal medical information about patients, the following types of illegal actions can be committed: improper collection of personal medical information by other people without legal grounds for its collection; improper distribution of personal medical information; improper use and improper storage of personal medical information.

Federal Law of July 27, 2006 No. 152-FZ "On personal data"[1] (further – the Law "On personal data") contains no reference rule on imposing criminal liability for divulgence of personal data. However, one should bear in mind that the problem of protecting biometric personal data is raised in many juridical sciences. At the same time, the issue is complicated by the fact that currently there is no common conceptual and categorical framework or legal regime, which causes problems in law enforcement, including those related to distinguishing between administrative law breaches and crimes.

From the viewpoint of conceptual and categorical framework, criminal legislation uses the notion "information about the private life of a person constituting their personal or family secret" (Article 137 of

[1] Federal Law of July 27, 2006 No. 152-FZ "On personal data". Collection of legislation of the Russian Federation. 2006. No. 31 (part I). Article 3451.

https://doi.org/ 10.54934/ijlcw.v1i2.29

the Russian Criminal Code) and "personal data" (part 2 of Article 173^2 of the Russian Criminal Code), administrative law – "restricted-access information", labor law – "personal data", civil law – "non-material values", medicine – "medical confidentiality". However, in our opinion, this may lead to problems in qualification of illegal actions, when it may be hard to distinguish between "restricted-access information" and "information about the private life of a person". We believe that in all branches of the Russian law there must be a common regime of personal data protection. Therefore, the above categories must be demarcated. Conversely, foreign authors strived to distinguish between information about the private life of a patient and other confidential information by specifying the main criterion for their distinction – they refer to different types of protection, which correspond to different types and methods of civil rights and interests' protection and have different accentuations (NanLiu, ShiyongChen, 2022).

According to Article 13 of Federal Law of November 21, 2011 No. 323-FZ "On the principles of health protection of the citizens in the Russian Federation", ***medical confidentiality*** is interpreted as *"information about the fact of a citizen applying for medical aid, condition of their health and diagnosis, other data obtained during their medical examination and treatment"*.

The legislative definition of "personal data" is contained in the Law "On personal data", which stipulates that "personal data are any information referring directly or indirectly to a particular or defined physical person (the subject of personal data)". It is worth noting that the definition of "personal data" is too abstract and allows referring *any data* to such (in the opinion of the subject). Besides, the law does not stipulate any specific list of data referred to personal data. Some definite interpretation may arise when examining Article 8 of the Law "On personal data", which stipulates that "the publicly available sources of personal data, with the written consent of the subject of personal data, may include their surname, first name, year and place of birth, address, telephone number, information on profession and other personal data, reported by the subject of personal data". However, of interest is the double blanket character, used in the above definition in relation to the notion of "other personal data".

In turn, medical confidentiality is closely connected with personal data, which, in our opinion, are its indispensable reflection. In judicial practice there are cases when criminal liability was imposed for disclosure of information about a patient's state of health, constituting medical confidentiality. *According to the Prosecutor's Office of Chelyabinsk oblast, a 46 year-old resident of Desyatiletiye village is charged with a crime stipulated by part 1 Article 137 of the Russian Criminal Code. In 2015, the woman, working*

https://doi.org/ 10.54934/ijlcw.v1i2.29

as a hospital attendant, in conversations with the village residents disclosed information about the state of health of a patient, which became known to her in relation with her employment duties[2].

According to the tenor of Article 3 of the Law "On personal data", the information constituting personal and family secret can be referred to the personal data. At that, personal and family secret constitute a large part of the volume of the notion of personal data. The Constitutional Court of the Russian Federation formulated in its Resolution of June 28, 2012 No. 1253-O: "... only the person themselves is entitled to determine which data referring to their private life must remain secret, therefore, collection, storage, use and dissemination of such information, not entrusted to anyone, is not allowed without consent of the said person, as is stipulated by the Constitution of the Russian Federation"[3].

Stemming from the carried out examination of judicial practice, one may conclude that personal data are characterized by the following features:

– *information about a person;*

– *the person determine by themselves, which data refer to their private life and, therefore, are a secret;*

– *the said data are not subject to control on the part of the state and the society;*

– *they are not of illegal character.*

Based on the above, one may assert that personal data shall constitute a personal and/or family secret in case the subject themselves refers them to such. That said, *a personal and family secret complies with all features of personal data* (though of a special nature). However, it is interesting to note that the said circumstance was not taken into account in the Decree of the Plenum of the Supreme Court of the Russian Federation of December 25, 2018 No. 46 "On some issues of judicial practice in cases on crimes against constitutional human and civil rights and freedoms (Articles 137, 138, 138[1], 139, 144[1], 145, 145[1] of the Russian Criminal Code)"[4].

[2] https://epp.genproc.gov.ru/ru/web/proc_74/mass-media/interviews-and-presentations

[3]Resolution of the Constitutional Court of the Russian Federation of June 28, 2012 No. 1254-O "On refusal to hear an appeal of Ukraine citizens Svetlana Vladimirovna Bondarkova, Aleksey Vasilyevich Zolin and Vasily Sergeyevich Zolin of violation of their constitutional rights by clause 'a' of Article 5, Article 6 and part 1 of Article 12 of Federal Law "On the citizenship of the Russian Federation". "KonsultantPlyus" Reference system.

[4] Decree of the Plenum of the Supreme Court of the Russian Federation of December 25, 2018 No. 46 "On some issues of judicial practice in cases on crimes against constitutional human and civil rights and freedoms (Articles 137, 138, 1381, 139, 1441, 145, 1451 of the Russian Criminal Code)". Rossiyskaya gazeta, January 9, 2019.

https://doi.org/ 10.54934/ijlcw.v1i2.29

2.2 Criminal law protection of personal data

The institute of personal data, medical confidentiality and information about the private life of a person constituting their personal or family secret is protected by criminal and administrative legislation of Russia.

In its explanation, the Supreme Court of the Russian Federation did not determine the list of data referred to personal or family secret or draw its difference from other categories, including personal data; hence, there are no criteria for distinguishing between criminal and administrative liability.

The institute of personal data is protected by administrative legislation, in particular Articles 13.11 and 13.14 of the Russian Administrative and Procedural Code. The objects of these administrative law breaches are public relations in the sphere of communication and information, which stems from the structure of the normative-legal act. Administrative liability must be imposed for the deeds which are less publicly hazardous than crimes. However, the character of public hazard of such deeds must cause no doubt, especially under the accelerating informatization of the society, emergence of new technologies, devices and techniques of obtaining, transmitting and storing of information.

In our opinion, a more consequential and substantiated approach is criminalization of the deeds related to the essential violation of the current legislation on personal data protection.

According to T. V. Deryugina, criminal legislation has a significant gap in the sphere of non-material values protection, being limited to two norms: Articles 137 and 128^1 of the Russian Criminal Code (Mokhov, 2021).

The objective part of corpus delicti stipulated by Artcile 137 of the Russian Criminal Code is liability for illegal collection or distribution of information about the private life of a person constituting their personal or family secret. It stipulates prohibition of *illegal collection of information*, but the list of means is not determined in the structure of Article 137 of the Russian Criminal Code; thus, it can be stated that the means of information collection may be both *unprohibited by law* (personal surveillance, questioning of persons), and *illegal* (theft, illegal trespassing, wiretapping, unsanctioned copying, etc.). Thus, liability depends on the means of collecting such data, as illegal means of collecting information may constitute a separate corpus delicti.

https://doi.org/ 10.54934/ijlcw.v1i2.29

At the same time, of interest is the legislative approach to constructing a criminal-legal norm stipulated in Article 183 of the Russian Criminal Code, which determines the means of collecting information constituting a commercial, banking, or taxation secret: theft of documents, bribery, threats, other illegal means. We believe that the indication of the "illegal" character of acquiring such data indicates the increased public hazard of the deed, the degree of such hazard being related to such means.

In general, many articles of the Russian Criminal Code stipulate liability for violation of various aspects of privacy (Art. 137, 138, 272 or 273 of the Russian Criminal Code). These components of cries only partially comprise the actions entailing the violation of rules of working with personal data. In our opinion, the "fragmentation" of the said norms cannot result in an efficient law and order maintenance in the sphere of personal data protection.

Thus, it is still unclear if the information about a private life of a person, constituting their personal or family secrecy, is personal data. And how may one distinguish the actions of distributing information (personal data), stipulated by Article 13.11 of the Russian Administrative Code, from the actions of distributing information about a private life of a person, constituting their personal or family secrecy (Article 137 of the Russian Criminal Code)?

Returning to the above said, we should note that the initial version of the Law "On personal data" stipulated the list of personal data including surname, name, patronymic, year, month day and place of birth, address, marital, social, property status, education, profession, income, and other information. However, this clarification is lacking in the present version. To resolve the said problems in the judicial and investigative practice we consider it necessary for the legislator to again stipulate the list of information constituting personal data.

The said list of data will help to distinguish the category of "personal data" from "information about a private life of a person, constituting their personal or family secrecy" and, respectively, administrative law breaches from crimes.

As the norms of administrative liability protecting personal data are currently insufficiently effective, we consider it necessary to stipulate criminal liability for unlawful processing of personal data of a citizen without their consent in case a significant harm is infringed upon their rights and legal interests.

https://doi.org/ 10.54934/ijlcw.v1i2.29

As a rule, the term "significant" is an evaluation category, which causes difficulties in qualification. We believe that a significant harm must be determined depending on what harm was infringed upon public relations, including material loss. Besides, in is necessary to stipulate in comments to Article 137 of the Russian Criminal Code, what will be interpreted as "significant harm".

2.3 Biometrical personal data: criminal legal risks

Criminal-legal protection of personal data, including biometric personal data, is necessarily and logically determined by the accelerated digitalization of public relations. In this regard, the Russian criminal law should take a special position in protecting such public relations from criminal infringements. One should agree with V. A. Chukreyev, who believes that unlawful trafficking of personal, including biometric, data is dangerous due to the fact that an intruder represents themselves as another person.

Biometric personal data serve as the indication of a legal subject, allowing an informational system to identify the specific subject, owner of digital rights.

According to Article 11 of the Law "On personal data", biometric data are the data referred to a specific person. These data indicate physiological and biological features of a person. We believe that this notion is disputable, as the notion "biological' is broader and includes physiological information.

Examination of the current components of crimes in the Special part of the Russian Criminal Code showed that it does not stipulate liability for. In our opinion, this circumstance is a legal gap of the legislator, due to the increased public danger of such deeds. The danger of biometric personal data falsification consists of two aspects. The first is the ability to commit fraud (Articles 159-159^3, 159^6 of the Russian Criminal Code) aimed at stealing other people's property, the second is the ability to obtain unlawful access to computer information (Articles 272 and 274 of the Russian Criminal Code).

Let us illustrate the above said with the following example. Such simple models of biometric data as papillary patterns of fingers (fingerprints), iris or their combination, can be falsified. To falsify a dactyloscopic record one should obtain the original etalon print – a biometric sample or its image. Then one must manufacture it with one of the methods depending on the operation mode of dactyloscopic scanner. Manufacturing contact lens with a fake iris is rather simple. There are Internet sites with

https://doi.org/ 10.54934/ijlcw.v1i2.29

instructions on manufacturing fake fingerprints and iris patterns[5]. Criminalization of such deeds would lead to blocking the resources which contain instructions on breaking biometric-based systems. Many specialists consider the issues of biobanks and data storage (Dankar, F.K., Ptitsyn, A.&Dankar, S.K., 2018).

We believe that manufacturing fake models of biometric personal data should be recognized as a publicly dangerous deed and stipulate liability for committing it, constructing the components of crime as the "formal" one, accomplished at the stage of manufacturing fake models of biometric personal data.

The proposal of criminalizing the components of crime indirectly stems from the Decree of the Russian Government of 6 July 2008 no. 512 "On adopting the requirements for material carriers of biometric personal data and technologies of storing such data outside of informational systems of personal data"[6], according to which the carriers of biometric personal data must provide protection against unsanctioned access, repeated or additional recording of information; it also stipulates the terms of exploitation of the carrier and the possibility to use the qualified electronic signature for maintaining the integrity and , целостности и inalterability of personal data.

At the same time, the public danger of falsifying biometric personal data is rather high and is expressed in infringement upon citizen's rights stipulated by Articles 23, 24, 34 and 35 of the Russian Constitution. Manufacturing, storing, transportation and marketing of falsified biometric personal data is undoubtedly a publicly dangerous deed. Such unlawful actions may serve as a preparatory stage for committing other crimes infringing upon the property of the digital economy actors, including unlawful access to computer information, fraud, forgery of passports contacting chips with biometric data.

A digital etalon model of biometric personal data per se is a *nonmaterial object*. Reproduction of a physical model of biometric personal data based on the digital etalon can be a difficult task. The use of fake biometric data in the digital space is partially covered by the norm of Article 272 of the Russian Criminal Code, while liability for the use of a reproduced physical model of biometric personal data is not

[5]https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%98%D0%B4%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F_%D0%BF%D0%BE_%D1%80%D0%B0%D0%B4%D1%83%D0%B6%D0%BD%D0%BE%D0%B9_%D0%BE%D0%B1%D0%BE%D0%BB%D0%BE%D1%87%D0%BA%D0%B5_%D0%B3%D0%BB%D0%B0%D0%B7%D0%B0

[6]Decree of the Russian Government of 6 July 2008 no. 512 "On adopting the requirements for material carriers of biometric personal data and technologies of storing such data outside of informational systems of personal data". Collection of legislation of the Russian Federation. 2008. N 28. Art. 3384.

https://doi.org/ 10.54934/ijlcw.v1i2.29

stipulated. A fake physical model can be used for unlawful access to information-telecommunication systems, mobile devices, payment systems, as well as to circumvent restrictions of access control systems, in future – to pass customs control. The use of fake biometric data may infringe property harm, and in cases of intrusion to secure facilities provoke failures in the information systems functioning, technological accidents and catastrophes.

Let us consider the position reflected in clause 1 of the resolution of the plenum of the Supreme Court of the Russian Federation of 17 December 2020 no. 43 "On some issues of judicial practice on the cases of crimes stipulated by Articles 324-327[1] of the Russian Criminal Code", according to which the "official documents, conferring the rights on or releasing from an obligation of, in Article 324 of the Russian Criminal Code, and the official documents in Part 1 of Article 325 of the Russian Criminal Code are such documents, including electronic ones, which are created, issued or verified in the order stipulated by law or other normative act by the federal bodies of state power, bodies of state power of the Russian Federation subjects, bodies of local self-government or authorized organizations or persons (educational, medical and other organizations regardless of the form of ownership, officials and persons executing managerial functions in commercial and non-commercial organizations, examination, medical and other commissions, notaries, etc.) and certify judicially significant facts"[7].

Biometric personal data, which are the main identifying sign in the Unified Biometric System, are not an electronic document, thus the deeds are not qualified according to Article 325 of the Russian Criminal Code. However, falsifying biometric personal data may lead to the consequences similar to Article 325 of the Russian Criminal Code.

Rather frequent are cases of fraud in which wrongdoers may obtain a legitimate (authentic) biometric sample of voice. For example, *in the city of Zelenograd, a criminal case was initiated after a theft from a bank card. A 40 year old local citizen received a telephone call from an unknown person who introduced himself as a bank employee and informed of unsanctioned attempts to write off the money from his cards. The fraudster managed to gain the man's trust by telling the contact data and card numbers, as well as the data from the reverse side of the cards; at that, he did not require any additional information, just asking to answer positively or negatively the question: "Do you agree to block the accounts of the*

[7] Resolution of the plenum of the Supreme Court of the Russian Federation of 17 December 2020 no. 43 "On some issues of judicial practice on the cases of crimes stipulated by Articles 324-327.1 of the Russian Criminal Code". Rossiyskaya gazeta, 30 December 2020.

https://doi.org/ 10.54934/ijlcw.v1i2.29

cards from which unknown persons attempted to write off the funds?" The victim answered "yes", after which he noticed money credited on his card and immediately written off together with his own savings. The overall loss amounted to over 68 thousand rubles[8]. The positive answer of the victim was later used during a session of distant bank servicing.

In the context of this example, it is interesting to note the statistics of banking operations, according to which in 2019 in the Russian Federation 576,566 operations were performed via electronic payment means without the clients' consent; 69% of such operations were performed by the clients themselves under the influence of fraud or abuse of trust[9], and the rest 31% by the wrongdoers obtaining unlawful access to the victims' electronic means of payment (Article 272 of the Russian Criminal Code) and further theft of money (Article 158 of the Russian Criminal Code).

Such cases are already not a matter of the distant future and demonstrate the need to react, including by legal means. For example, in China wrongdoer deceived the personality checking system of the taxation service and falsified consignment bills since 2018. Fraudsters purchased high-quality photos and fake personal data. Using false photos and applications turning photos into videos, they managed to deceive the national face-recognition system. The image is processed so that the photo "moves"; a video is created, which contains the needed actions, including nodding and head shaking, winking, opening the mouth. The fake video was loaded to the especially cross-flashed smart phone. During personality identification, the frontal camera of the gadget was not switched on; instead, the system "saw" the specially produced video. The fraudsters forwarded fake invoices from a fake company, hoping the forgery would not be noticed and the invoices would be paid. In two years, the wrongdoers managed to earn about 57.5 million rubles[10].

In case the Unified Biometric System is contaminated with malware, there are signs of a crime stipulated by Article 273 of the Russian Criminal Code, when the object of crime is the body of public relations of lawful and safe use of the protected computer information. The objective part is the creation of a computer program intended for destruction or modification of the personal data samples stored in the Unified Biometric System.

[8] https://www.zelao.ru/55/540/44070-politsiya-zelenograda-prosit-byit-bditelnyimi-pri-postuplenii-lyubyih-zvonkov-iz-bankov-/

[9] Review of operations committed without the consent of the clients of financial organizations in 2019, prepared by the Central Bank of the Russian Federation. https://www.cbr.ru/Collection/Collection/File/32190/Review_of_transactions_2020.pdf

[10] https://ru-bezh.ru/gossektor/news/21/04/05/s-pomoshhyu-obyichnogo-foto-dva-zhitelya-kitaya-obmanuli-naczion

https://doi.org/ 10.54934/ijlcw.v1i2.29

3. CONCLUSIONS

Ah! ***First***, the institution of personal data, including biometric personal data, is broader than the institution of medical secrecy and includes a broader range of information about a patient. This is due to the fact that the institution of personal data is universal, as it is aimed at regulating public relations in various spheres of public life, while the institution of medical secrecy – in the healthcare system only (has a narrower sphere of action). Consequently, the provisions on personal data protection and their high vulnerability are applicable to all spheres of regulating public relations, not only the relations arising in healthcare.

Second, the title of Article 137 of the Russian Criminal Code should be changed for "Violation of privacy and legislation of the Russian Federation on personal data".

Third, criminal liability should be established for unlawful processing of other personal data which infringed significant harm upon the rights and legal interests of a person, the disposition of the criminal-legal norm being formulated as follows:

"1. Unlawful collection or distribution of information about the private life of a person constituting their personal or family secrecy without their consent or infringing significant harm upon the rights and legal interests of the person as a result of unlawful processing of other personal data, or distribution of this information in a public report, publicly demonstrated work of art or in mass media or in "the Internet" information-telecommunication network...".

Fourth, taking into account a high public danger of the deeds which can be committed using biometric personal data and their value, we consider it necessary to criminalize the components of crime consisting in *manufacturing and (or) marketing of fake models of biometric personal data.*

The said components of crime should be recognized as a publicly dangerous deed and considered as formal components of crime, accomplished at the stage of manufacturing and (or) marketing. We believe that it should be placed within Article 137^1 of Chapter 19 "Crimes against constitutional rights and freedoms of a human and a citizen" of the Russian Criminal Code. Such placement of the components of crime, stipulated by Article 137^1 of the Russian Criminal Code, is determined by the object of criminal-legal protection, which are primarily the constitutional rights of a person.

Fifth, the criminal-legal norm protecting privacy as a constitutional principle does not stipulate the increased liability for distribution of databases (informational systems of personal data) containing, for instance, a medical secrecy, which do not refer to a commercial or banking secrecy, hence, such unlawful actions do not entail liability according to Article 183 of the Russian Criminal Code. We believe that

https://doi.org/ 10.54934/ijlcw.v1i2.29

Article 137 of the Russian Criminal Code must also stipulate a prohibition of unlawful distribution of information systems (or electronic information resources), which contain personal data with restricted access.

Sixth, the protection of biometric personal data should be given more attention compared to personal data, due to their high vulnerability. In this connection, the issues of processing and storing of biometric data should be paid special attention, as their loss may lead to grave consequences. The loss of such data compared to documents cannot be changed, unless an operation is performed.

REFERENCES

[1] Alrefaei, A.F., Hawsawi, Y.M., Almaleki, D., et al. (2022). Genetic data sharing and artificial intelligence in the era of personalized medicine based on a cross-sectional analysis of the Saudi human genome program. *Sci Rep* 12, 1405. https://doi.org/10.1038/s41598-022-05296-7.

[2] Chukreev, V. A. (2022). Personal biometric data as subjects of criminal law protection. *Courier of Kutafin Moscow State Law University (MSAL).* 2022;(3):107-116. (In Russ.) https://doi.org/10.17803/2311-5998.2022.91.3.107-116

[3] Dankar, F.K., Ptitsyn, A., and Dankar, S. K. (2018). The development of large-scale de-identified biomedical databases in the age of genomics – principles and challenges. *Hum Genomics* 12, 19. https://doi.org/10.1186/s40246-018-0147-5.

[4] Istratova, E.E., Molchanov, A.A. (2015). Features of personal data protection in medical information systems. *Journal of Siberian Medical Sciences*. no. 6. p. 59.

[5] Kichko, K., Marschall, P., and Flessa, S. (2016). Personalized medicine in the US and Germany: awareness, acceptance, use and preconditions for the wide implementation into the medical standard. *J. Pers. Med.* 6(2), E15. https://doi.org/10.3390/jpm6020015 .

[6] Lopes, I. M., Guarda, T., and Oliveira, P. (2020). General Data Protection Regulation in Health Clinics. *J Med Syst* 44, 53. https://doi.org/10.1007/s10916-020-1521-0.

[7] Mitchell M., Kan L. (2019). Digital Technology and the Future of Health Systems. *Health Systems & Reform*, no. 5:2. pp. 113-120, https://doi.org/10.1080/23288604.2019.1583040.

[8] Mokhov, A. and Sushkova, O. (2021). *Legal foundations of bioeconomics and biosafety*: monograph. Moscow: Prospekt. pp. 225. DOI 10.31085/9785392310944-2020-480.

[9] Molchanov, A. E., Molchanov, A.A. (2015). Features of personal data protection in medical information systems. *Siberian Medical Journal*, no. 6, p. 59.

[10] Nan Liu, Shiyong Chen (2022). The Protection Mechanism of Personal Health Information in the Digital Economy Environment. *Hindawi Journal of Environmental and Public Health*, Article ID 2314468, https://doi.org/10.1155/2022/2314468.

[11] Raimundo, G. C., Grando, L. L., Machado, ANC, Oliveira, M., and Cabar, F. R. Ethical and bioethical aspects concerning the disclosure of medical information for a fair reason. *Rev Assoc Med Bras* (2022). Feb; 68(2). pp. 202-205. doi: 10.1590/1806-9282.20211043.

ABOUT THE AUTHOR

Albina Shutova – Ph.D. in Law. Senior Researcher of the Institute of Digital Technologies and Law. Associate Professor at Department of Criminal Law and Procedure, Kazan Innovative University named after V.G. Timiryasov, Kazan, Russian Federation.
e-mail: mailto:Shutova1993@inbox.ru

ABOUT THIS ARTICLE

Conflict of interests: Author declare no conflicting interests

https://doi.org/ 10.54934/ijlcw.v1i2.29