Issues of personal data protection through the lens of sustainable development and law

Ildar Begishev[1,*], *Mehrdad Rayejian* Asli[2], *Veronika* Denisovich[3], *Andrey* Majorov[3], and *Andrey* Sergeyev[3]

[1]Kazan Innovative University named after V.G. Timiryasov, Moskovskaya str., 42, 420111, Kazan, Russia
[2]Institute for Research and Development in the Humanities, Al-e-Ahmad Highway, Yadegar Bridge, 1463645851, Tehran, Iran
[3]Chelyabinsk State University, Brothers Kashirin str., 129, 454001, Chelyabinsk, Russia

Abstract. The paper focuses on the effectiveness of legislation regulating the security of storage, processing, and transfer of personal data. As the main thesis, we assume that it is necessary to give a legal definition of the concept of personal data to build specific legal norms of a protective nature. We describe, examine, and evaluate the provisions of international regulatory legal acts that define the concept mentioned above and correlate with Russian legislation provisions. We thoroughly consider the opinions of scientists on the issue with the justification of our assessments and judgments. The results of the study can be considered recommendations on understanding the definition of personal data, as well as proposals for their protection and development of the system of legal regulation of personal data turnover in various jurisdictions.

Keywords: sustainable development, security, cybercrime, personal data, law, legal regulation, crime.

1 Introduction

In the context of forming a digital society [1], a significant amount of data about an individual is placed in networks [2-7]. This pattern is obvious and does not require confirmation. Information about private life [8], details of bank cards and other payment instruments [9], the location of owners of digital devices are widely distributed on the internet, which creates recognized criminological risks, including in the context of the use of AI [10]. The practice of sharing personal data can be improved [11]; it needs more detailed regulation [12].

Problematic issues of law enforcement arise when using software and hardware products with user geolocation data [13, 14]. Reasonable judgments are made about their belonging to personal data and the need to obtain the subject's consent for their use [15]. There is also a gap in the legal regulation of the use of personal data of patients in the provision of medical services [16]. Many authors justify the need for the special legal protection of this type of personal data, since they are related to intimate aspects of the personal life of the subject [17, 18].

* Corresponding author: begishev@mail.ru

These facts raise the idea of comprehensive protection of personal data through the definition of the concept and the addition of criminal legislation with appropriate features. This is an important issue for the legal system that requires a speedy solution.

2 Materials and Methods

In this study, combinations of various methods of scientific cognition were used, which made it possible to achieve such results. Each postulate, scientific opinion, and legislative position under study is subjected to rational critical thinking, which is the basis of spectral testing. Besides, we used the secondary literature and the provisions of normative legal acts.

3 Results

The definition of personal data in the Federal Law "On Personal Data" [19] and the Federal Law "On Information, Informatization and Information Protection" [20] have different positions on this issue. However, with the passage of time and the development of domestic legislation, the concept of personal data has become broader and includes any information that directly or indirectly relates to a specific individual. This definition includes information about facts, events and circumstances of citizens' lives that can be used to identify them.

According to your opinion, the definition of "personal data" in the current legislation has a high level of abstraction, which can lead to a broad classification of any information related to a person. You point to Article 8 of the Federal Law "On Personal Data", which provides relative specifics regarding publicly available sources of personal data. This article allows you to include in such sources the surname, first name, patronymic, year and place of birth, address, subscriber number, information about the profession and other personal data provided by the subject of personal data on the basis of written consent. However, it should be borne in mind that the legislation on the protection of personal data develops and is supplemented over time in accordance with changing technologies and social realities. The above-mentioned provisions may be clarified to provide a more precise definition of personal data and their use.

It seems to us that the problem of defining and using information about legal entities in the context of information and personal data protection is of the most important legal importance. In fact, personal data legislation usually focuses on information related to individuals, since personal data is primarily associated with specific individuals. However, in some cases, information about legal entities may also be considered confidential or requiring protection. As for the concept of "information that must be kept secret", this is a kind of general concept that is not always explicitly defined in federal legislation. It is important here to provide a legal norm or context in which this concept is used in order to better understand its legal certainty and interpretation. The development of clear and consistent legislation regarding the protection of information and personal data is a complex task that requires taking into account many factors and the needs of various subjects of law. Thus, it can be the subject of further legal discussions and judicial practice to clarify and resolve emerging issues.

Scientists suggest that the definition of personal data cannot be fully described by the above facts, and argue that the use of excessive abstraction in legal definitions may be acceptable for industry legislation, but inappropriate when constructing elements of a crime and fixing them in criminal law. Thus, we conclude that it is impossible to implement a concept that suggests a transition to an independent formulation of the legal definition of personal data. Despite this, the definition of the concept of personal data reflected in the law faces serious problems related to the final formulation of the concept in scientific research.

Consequently, some researchers interpret personal information (personal data) as "facts, reports, and opinions that relate to a given person and that could be expected to be considered intimate and confidential; and therefore want to stop or at least limit its dissemination" [21]. We believe that this definition is not entirely successful, since the attribution of personal information to all data makes them broader and requires attribution of the entire spectrum of such data.

Some researchers believe that the definition should include "confidential information of a citizen". We believe that there are no sufficient grounds to consider this proposal constructive. The potential for abstracting this phrase exceeds the formal interpretation of the concept of personal data, which does not meet the requirements of legal certainty of legal regulation and entails the inability of citizens to behave following the requirements of regulatory legal acts. "Similar opinions are expressed about the ability of the subjects of personal data to determine which information about their identity is general, that is, available for review, copy, and use by an indefinite number of persons, and which are subject to state protection" [22].

We do not share this opinion either, since the subject of personal data is not always able to independently assess the significance of personal data and make a decision on their classification. In this context, we note the predominance of these positions and the diversity of criteria for classifying personal data [23]. In any case, opinions based on the need to delegate the authority to select protected personal data directly to the personal data subject are deconstructive.

Also, we draw attention to the opinions of researchers who indicate the need to involve international legal mechanisms for the protection of personal data [24]. We express our opinion on the expediency of using international mediation methods. There are no sufficient grounds to regard this position as justified; the use of such legal practice contradicts the national sovereignty of the country in the application of legislation.

The positive assessments of the Korean legislation in the field of personal data, which establish legal mechanisms for controlling the process of using personal data by providing consent to their storage, processing, and transfer, are entirely justified [25]. We are sure about the correctness and consistency of the legislator's position, which is expressed in the establishment of categories of personal data, concerning which the subject of personal data applies differentiated control measures.

The scientist from the United States sufficiently disclosed the issue of distinguishing categories of personal data. They logically and reasonably substantiated the need for the special legal protection of the part of the personal data that discloses the circumstances of providing medical care to a person. At the same time, they indicated that such issues are not given due importance in legal practice [26]. Japanese scientists have similar positions [27]. Moreover, many scientists share this position, which prevails in the international secondary literature [28].

4 Discussion

Among the proposals for improving personal data protection, we regard the authors' claims about the need to provide technical means of protection for automated control systems where personal data is circulated as reasonable [29]. Indeed, the technical aspects of data protection are essential. We consider this position as the central thesis.

In this context, the proposals on using blockchain technology in the design of technical means of personal data protection are of scientific interest [30]. However, we disagree with this position. In terms of legal regulation, it would be more appropriate not to limit the list of technical means of information protection only to blockchain technologies, delegating specific means of protection directly to the user or operator of personal data they get certain freedom of action. At the same time, it is necessary to take into account the pace of development of digital technologies [31-41].

The issues of the correlation between the protection of personal data and the functioning of automated security systems operating in the interests of ensuring anti-terrorist security, considered by European researchers, are extremely relevant [42]. We believe that social and national security from terrorist attacks is much more significant than the interests of protecting personal data. Moreover, verification by authorized bodies excludes the possibility of misuse of personal data.

Indeed, it is unlikely to fully describe the concept of personal data as a feature that characterizes the subject of a crime, since the latter cannot be normalized.

5 Conclusions

Summing up the results of the study, we will draw some conclusions regarding the solution of personal data protection issues through the prism of sustainable development and law, among which we can highlight the main:

- Causing death to the subject of personal data;
- Causing serious or actual bodily injury to the subject of personal data;
- Destruction or damage of the personal data subject's property;
- Violation of the personal confidentiality of the subject of personal data;
- Dissemination of information discrediting personal data subjects or their relatives.

References

1. D.A. Pashentsev, M.V. Zaloilo, O.A. Ivanyuk, D.R. Alimova. Digital technologies and society: Directions of interaction. Revista ESPACIOS, **40(42),** 1-6 (2019).
2. D. Cyman, E. Gromova, E. Juchnevicius. Regulation of artificial intelligence in brics and the European Union. BRICS Law Journal, **8(1),** 86-115 (2021).
3. A. Zharova. Introducing artificial intelligence into law enforcement practice: The case of Russia. Annals of DAAAM and Proceedings of the International DAAAM Symposium, **30(1),** 688-692 (2019).
4. I.R. Begishev. Limits of criminal law regulation of robotics. Vestnik Sankt-Peterburgskogo Universiteta. Pravo, **12(3),** 522-543 (2021).
5. A.Y. Bokovnya, Z.I. Khisamova. Pressing issues of unlawful application of artificial intelligence. International Journal of Criminology and Sociology, **9**, 1054-1057 (2020).
6. A.A. Shutova, D.D. Bersei, E.V. Nechaeva. Bioprinting medical devices: Criminal evaluation issues. AIP Conf. Proc., **2701**, 020032 (2023). doi: 10.1063/5.0121700
7. I.A. Filipova. Neurotechnologies: Development, practical application and regulation. Vestnik of Saint Petersburg University. Law, **3**, 502-521 (2021). doi: 10.21638/spbu14.2021.302
8. M. Phillips, B.M. Knoppers. Whose commons? Data protection as a legal limit of open science. The Journal of Law, Medicine & Ethics, **47(1),** 106-111 (2019). doi: 10.1177/1073110519840489
9. A.Y. Bokovnya, A.A. Shutova, T.G. Zhukova, L.V. Ryabova. Legal measures for crimes in the field of cryptocurrency billing. Utopia y Praxis Latinoamericana, **25**(Extra7), 270-275 (2020).
10. I.A. Filipova. Artificial Intelligence Strategy and consequences of its implementation for labour law. Vestnik Sankt-Peterburgskogo Universiteta. Pravo, **13(1),** 5-27 (2022).

11. A. Zharova. The protect mobile user data in Russia. International Journal of Electrical and Computer Engineering, **10(3),** 3184-3192 (2020). doi: 10.11591/ijece.v10i3.pp3184-3192
12. P.A. Deverka, M.A. Majumder, A.G. Villanueva, A. Anderson, M. Bakker, A. Bardill. Creating a data resource: What will it take to build a medical information commons? Genome Medicine, **9(84),** 25-75 (2019). doi: 10.1186/s13073-017-0476-3
13. N.N. Chernogor, A.S. Emelyanov, M.V. Zaloilo. Genesis of post-modern: To the question of functional identification in law. Voprosy Istorii, **6(1),** 185-194 (2021).
14. E.A. Gromova, N.S. Koneva, D.B. Ferreira. Preferential and experimental legal regimes for the creation of innovative biomedical technologies. Human Sport Medicine, **21,** 161-166 (2021). doi: 10.14529/hsm21s223
15. R. Arthur, H.T.P. Williams. Scaling laws in geo-located Twitter data. PLoS ONE, **14(7),** e0218454 (2019). doi: 10.1371/journal.pone.0218454
16. I.R. Begishev. Criminal-Legal Protection of Robotics: Notion and Content. International Journal of Law in Changing World, **1 (2),** 73-83. (2022). doi: 10.54934/ijlcw.v1i2.33
17. C. Garattini, J. Raffle, D.N. Aisyah, F. Sartain, Z. Kozlakidis. Big data analytics, infectious diseases, and associated ethical impacts. Philosophy & Technology, **32(1),** 69-85 (2019). doi: 10.1007/s13347-017-0278-y
18. D. Utegen, B. Rakhmetov. Facial Recognition Technology and Ensuring Security of Biometric Data: Comparative Analysis of Legal Regulation Models. Journal of Digital Technologies and Law, **1(3),** 825-844 (2023). doi: 10.21202/jdtl.2023.36
19. Russian Federation. Federal Law "On Personal Data" (July 27, 2006 No 152-FL), (2016).
20. Russian Federation. Federal Law "On Information, Informatization and Information Protection" (February 20, 1995 No 24-FL), (1995).
21. R. Wacks. The protection of privacy. London, UK: Sweet & Maxwel, 1980.
22. D. Tegbaru, L. Braverman. ASTRO journals' data sharing policy and recommended best practices. Advances in Radiation Oncology, **4(4),** 551-558 (2019). doi: 10.1016/j.adro.2019.08.002
23. A.G. Villanueva, R. Cook-Deegan, B.A. Koenig, P.A. Deverka, E. Versalovic. Characterizing the biomedical data-sharing landscape. The Journal of Law, Medicine & Ethics, **47(1),** 21-30 (2019). doi: 10.1177/1073110519840481
24. S. Dewi, R. Walters, L. Trakman, B. Zeller. The role of international mediation in data protection and privacy law – can it be effective? Australian Dispute Resolution Journal, **61,** 19-77 (2019). doi: 10.2139/ssrn.3462113
25. S. Huh. Protection of personal information in medical journal publications. Neurointervention, **14(1),** 1-8 (2019). doi: 10.5469/neuroint.2019.00031
26. G. Demiris, S.-Y. Lin, A.M. Turner. The role of personal health information management in promoting patient safety in the home: A qualitative analysis. Assistive Technology Research Series, **264,** 1159-1163 (2019). doi: 10.3233/shti190408
27. S. Tashiro. Different uses of personal health information and its protection: From medical use to commercial use. Neurological Surgery, **47(2),** 241-248 (2019). doi: 10.11477/mf.1436203924
28. B.M. Knoppers. Framework for responsible sharing of genomic and health-related data. The HUGO Journal, **8(1),** 25-48 (2014). doi: 10.1186/s11568-014-0003-1

29. N. Anciaux, P. Bonnet, L. Bouganim, B. Nguyen, P. Pucheral. Personal data management systems: The security and functionality standpoint. Information Systems, **80**, 13-35 (2019). doi: 10.1016/j.is.2018.09.002
30. P. Esmaeilzadeh, T. Mirzaei. The potential of blockchain technology for health information exchange: Experimental study from patients' perspectives. Journal of Medical Internet Research, **21(6),** e14184 (2019). doi: 10.2196/14184
31. N.A. Alexandrova, T.Yu. Ksenofontova, E.A. Zharkova, V.A. Alexandrov, V.S. Kukhar. It staff turnover: Causes and management tools. E3S Web Conf., **395,** 05010 (2023). doi: 10.1051/e3sconf/202339505010
32. E.M. Akhmetshin, D.I. Stepanova, I.Y. Andryushchenko, H.A. Hajiyev, O.M. Lizina. Technological stratification of the large business enterprises' development. Journal of Advanced Research in Law and Economics, **10(4),** 1084-1100 (2019). doi: 10.14505/jarle.v10.4(42).10
33. D.D. Soloveva. Victimological Characteristics of Crimes Related to the Violation of Copy-right and Related Rights. Viktimologiya [Victimology], 2021, **8(2),** 170-182 (2021).
34. R. Sharafutdinov, V. Gerasimov, E. Akhmetshin, H. Okagbue, A. Tagibova. State digitalzation policy as a factor of sustainable inclusive growth and development of russian regions. Paper presented at the E3S Web of Conferences, **208** (2020). doi: 10.1051/e3sconf/202020808031
35. O. Saidmamatov, U. Matyakubov, E. Khodjaniyazov, J. Day, E. Ibadullaev, S. Chuponov, D. Bekjanov, M. Matniyozov, B. Matyusupov. TOWS analysis for sustainable ecotourism development and state support during the pandemic: The Aral sea region of Uzbekistan. Turyzm/Tourism, **31(1)**, 47-56. (2021). doi:10.18778/0867-5856.31.1.16
36. I.S. Abdullaev, P.A. Gurbanov, R.A. Aleshko, Y.Yu. Finogenov. Improvement of the organizational and economic mechanism of innovative development of the food and processing industry. Siberian Journal of Life Sciences and Agriculture, **15(3),** 357-386 (2023). doi: 10.12731/2658-6649-2023-15-3-357-386
37. D. Hudayberganov. Evaluation and perfecting mechanisms of increasing the effectiveness of the goods and services market. Journal of Critical Reviews, **7(1),** 512-516(2020).
38. A.N. Khomenko. On the Victimization of Cybercrime Victims. Viktimologiya [Victimology], **8(2),** 143-148 (2021).
39. K. Bagratuni, E. Kashina, E. Kletskova, D. Kapustina, M. Ivashkin, V. Sinyukov, A. Karshalova, H. Hajiyev, E. Hajiyev. Impact of socially responsible business behavior on implementing the principles of sustainable development (experience of large business). International Journal of Sustainable Development and Planning, **18(8),** 2481-2488 (2023). doi: 10.18280/ijsdp.180819
40. M.A. Bazhina. Intelligent Transport Systems as the Basis of de Lege Ferenda of the Transport System of the Russian Federation. Journal of Digital Technologies and Law, **1(3),** 629-649 (2023). doi: 10.21202/jdtl.2023.27
41. M. Kerimov, V. Smelik, M. Kerimov, M. Volkhonov, V. Kukhar. Nanotechnologies in agricultural engineering: practice and prospects, E3S Web of Conf., **222,** 01022 (2020). doi: 10.1051/e3sconf/202022201022
42. S. Matos. Privacy and data protection in the surveillance society: The case of the prüm system. Journal of Forensic and Legal Medicine, **66**, 155-161 (2019). doi: 10.1016/j.jflm.2019.07.001