

CRIMINAL LAW PROTECTION OF PERSONAL DATA IN A DATA ECONOMY****Albina A. Shutova, Ildar R. Begishev, Anna V. Volkova***Kazan Innovative University named after V.G. Timiryasov, Kazan, Russia***Article info**

Received –

2026 January 13

Accepted –

2026 March 20

Available online –

2026 June 20

Keywords

Personal data, data economy,
criminal liability, illegal trafficking
of personal data, information
security, corpus delicti,
digitalization, criminalization,
information society

The article addresses a subject of acute contemporary significance: the criminal law protection of personal data under conditions of an emerging data economy.

The research hypothesis advanced by the authors posits that, while the enactment of Article 272¹ of the Criminal Code of the Russian Federation represents a qualitatively new stage in the evolution of criminal law protection of personal data, the legislative construction of this norm contains substantial conceptual and technical deficiencies that impede effective law enforcement and require systematic legislative correction. The stated aim of the study – to determine the mechanism of criminal law protection of personal data in a data economy, assess the effectiveness of the new legislative instrument, and formulate proposals for its improvement – is declared as fully achieved by the authors.

The methodological framework of the study integrates general scientific methods – dialectical, systemic-structural, formal-logical, analytical and synthetic approaches – with specialised legal methods, including comparative law, formal dogmatic analysis and statutory interpretation.

The principal results of the research are structured across several interrelated dimensions. First, the authors examine the legal nature of personal data as the subject matter of criminal offences, demonstrating that, within the data economy paradigm, personal information acquires characteristics fundamentally distinguishing it from traditional objects of legal protection: it may be reproduced, aggregated and enriched without apparent detriment to the original subject, which substantially complicates the criminal qualification of unlawful acts. Second, the paper provides a systematic analysis of the corpus delicti under Article 272¹, identifying the constituent elements of its subject matter – computer information, the personal data content thereof, and the illegal origin of such information – as a tripartite construct that is unique within Russian criminal law and demands careful doctrinal elaboration. Third, the authors critically examine the legislative placement of Article 272¹ within Chapter 28 of the Criminal Code (crimes in the sphere of computer information), arguing that the primary object of the offence is not computer security but rather the constitutional right of the individual to privacy, personal and family secrecy as guaranteed by Article 23 of the Constitution of the Russian Federation, thereby supporting the position that normative placement within Chapter 19 would be more doctrinally coherent. Fourth, the study conducts a rigorous analysis of qualification problems arising from competition between Article 272¹ and related criminal law provisions, including Articles 137, 183, 272 and 274¹ of the Criminal Code, proposing specific rules for resolving such conflicts in practice.

The authors propose a normative clarification of the concept of “illegal acquisition” of personal data by way of a cross-reference to the grounds established by Federal Law No. 152-FZ on Personal Data; and the introduction of an immunity provision within the footnotes to Article 272¹ for persons who voluntarily disclose unlawfully obtained data arrays, modelled on analogous incentive norms elsewhere in the Criminal Code.

** The article was prepared with the scholarship support of the Kazan Innovative University named after V.G. Timiryasov (IEML).

1. Introduction

Society is undergoing a large-scale transformation due to the universal digitalization of economic, social and political processes. Information, primarily personal data of individuals, becomes a central element of economic activity, determining the competitiveness of market participants and forming an independent segment of the economy – the so-called data economy. This model of economic relations involves the large-scale collection, processing, storage and commercial exploitation of information about citizens, which inevitably creates new threats to their rights and legitimate interests [1]. It is important that the value of personal data as an economic asset is steadily increasing: it is used to build mechanisms for targeted advertising, credit scoring, medical diagnostics, as well as increasingly sophisticated schemes of fraud and other criminal attacks.

Statistics in this field is notable. According to analytics, in 2024, the volume of officially identified personal data leaks in Russia exceeded 1.5 billion records, and the total economic damage from such incidents was estimated at billions of rubles¹. These figures indicate that the illegal trafficking of personal data has become a large-scale socially dangerous phenomenon that threatens not only the rights of citizens, but also the stability of the state information infrastructure. Moreover, these crimes often serve as a tool for other criminal attacks – fraud, extortion, espionage – which indicates a high degree of their public danger.

Issues of personal data legal protection were repeatedly discussed in science [2–5]. In 2024, E.V. Khokhlova defended her Cand. Sci.

thesis in Criminal Law entitled “Illegal actions with personal data: criminal law research” [6]. However, the issue of criminal law instruments for countering the illegal personal data trafficking has become particularly acute only in recent years, due to fundamental changes in the system of both actual threats and legal regulation in this area. The starting point for the analysis is Federal Law No. 421-FZ² of November 30, 2024, which supplemented Chapter 28 of the Russian Criminal Code (hereinafter referred to as CC RF) with Article 272¹. It criminalized the illegal trafficking of computer information containing personal data. This step of the legislator generates a wide discussion and requires a multi-faceted theoretical and applied comprehension.

The problem of responsibility for the illegal trafficking of personal data is of particular interest to researchers. Many published works study the new corpus delicti provided for in Article 272¹ of the CC RF, as well as the problems of qualifying this crime [7–14]. Also, I.S. Alikhadzhieva published a series of works devoted to personal data as a specific area of crimes [15–18]. However, personal data in economic conditions were not studied so thoroughly.

It is worth paying attention to the fact that there is still no significant practice of applying these criminal law norms. According to the Russian Ministry of Internal Affairs, in the first half of 2025, 601 crimes under Article 272¹ of the CC RF were detected in Russia; criminal cases were initiated in 313 of them³. However, according to

² Federal Law No. 421-FZ of November 30, 2024 “On Amendments to the Criminal Code of the Russian Federation”. Collection of legislation of the Russian Federation. 2024. No. 49 (part IV). Art. 7412.

³ In six months, more than 600 crimes related to personal data trafficking were identified. URL: <https://ru-bezh.ru/zakonodatelstvo-i-normativyi/news/25/09/05/za-polgodu-vyyavili->

Law Enforcement Review

2026, vol. 10, no. 2, pp. 127–136

¹ InfoWatch: in 2024, Russia ranked five by the amount of leaked personal data. URL: <https://tass.ru/obschestvo/23439577> (access date: 12.01.2026).

the Judicial Department of the Russian Supreme Court, in the first half of 2025, only one citizen was convicted in such a case⁴. We believe that this fact should not hinder the comprehension of the corpus delicti provided for in Art. 272¹ of the CC RF, in order to forecast its application that may be useful for practice.

The objective of this study is to determine the mechanism of criminal law protection of personal data in the context of the data economy, including to evaluate the effectiveness of new legislative tools and to develop proposals for their improvement.

1. Personal data under the data economy

The data economy is a system of economic relations in which information about individuals and other information serve as a resource for producing value; that is, information has an economic value of its own [19, pp. 144–145]. This model relies on technologies like big data, artificial intelligence and machine learning, which allow extracting commercially significant insights from arrays of personal information collected during continuous monitoring of user behavior. Notably, in the data economy, personal data acquire features that fundamentally distinguish them from traditional objects of legal protection: they can be reproduced, aggregated and enriched without obvious damage to the original “carrier”, which significantly complicates the qualification of illegal actions with them.

Article 3 of Federal Law No. 152-FZ of July

27, 2006 “On Personal Data”⁵ (hereinafter referred to as Law No. 152-FZ) very broadly defines personal data as “any information relating directly or indirectly to a specific or identifiable natural person”. The lack of a specific list of information related to personal data leads to the fact that they include identifying information: name, address, document numbers, as well as indirect identifiers: biometric data, network identifiers, geolocation tags, and behavioral profiles⁶. This definition has an unacceptable level of legislative abstraction, which allows including any information related to a person in this category [2. P. 12]. The absence of a list of information related to personal data raises the question of their separation from information about a person’s private life that constitutes their personal or family secret (the scope of crime under Article 137 of the CC RF) [3. P. 334].

In turn, the scope of crime under Article 272¹ of the CC RF is not personal information as such, but computer information containing personal data obtained illegally. In the disposition of the criminal law norm, the legislator simultaneously uses the categorical apparatus of two legal regimes – information law and criminal law. This generates a number of qualification difficulties, which will be discussed further.

For law enforcement purposes, computer information containing personal data should be understood as numeric codes suitable for subsequent processing in information and

⁵ Federal Law No. 152-FZ of July 27, 2006 “On Personal Data”. Collection of legislation of the Russian Federation. 2006. No. 31 (part I). Art. 3451.

⁶ Clarifications of the Federal Service for Supervision of Communications, Information Technologies and Mass Communications dated August 30, 2013. “Clarifications on the issues of attributing photo, video, fingerprint data and other information to biometric personal data and the specifics of their processing”.

bole-600-prestupleniy-s-оборотom-personalny (access date: 12.01.2026).

⁴ Summarized statistical data on criminal records in Russia for the first half of 2025. URL: <https://cdep.ru/index.php?id=79&item=9303> (access date: 12.01.2026).

telecommunication systems, networks and devices and allowing identification of a specific person.

2. System of criminal law protection of personal data

Prior to the adoption of Federal Law No. 421-FZ of November 30, 2024⁷, criminal law ensured the protection of personal information of citizens through a number of norms in various chapters of the CC RF, which was confirmed by established law enforcement practice. First of all, this is Article 137 of the CC RF, which stipulated liability for the illegal collection or dissemination of information about a person's private life that constitutes their personal or family secret. In addition, Articles 138, 155, 183, 272, and 273 of the CC RF, as well as a number of other norms, performed protective functions in relation to certain categories of personal data. Nevertheless, these standards did not provide for the systematic criminal protection of personal data in their modern understanding, which is typical for the data economy. Article 137 of the CC RF focuses primarily on the protection of privacy in its traditional sense and does not cover numerous cases of mass commercial "exploitation" of personal data.

Of particular scientific and practical interest is Article 272¹ of the CC RF, which prohibits the illegal trafficking of computer information containing personal data. Its legislative structure contains a number of inaccuracies and legal uncertainties that can significantly complicate its practical application. In particular, the concept of "illegal receipt" of personal data needs to be clarified, since it is important for qualifying subsequent actions as

criminal. At the same time, Law No. 152-FZ provides for a significant list of grounds for the lawful processing of personal data without their subject's consent. This creates additional difficulties in distinguishing legitimate and illegal behavior in the field of data trafficking.

3. Corpus delicti provided for in Art. 272¹ of the CC RF: disputable issues

The correct identification of the object and scope of crime provided for in Article 272¹ of the CC RF is particularly important due to the complex legal nature of personal data and the ambiguous position of the legislator regarding the structure of protected legal relations. This provision is included in Chapter 28 of the CC RF, which implies that their generic object is classified as public safety and public order (Section IX of the CC RF), and the specific object is classified as public relations in the field of the safe use of computer information. However, illegal trafficking of personal data primarily encroaches on the constitutional right of citizens to privacy, personal and family secrets, guaranteed by Article 23 of the Russian Constitution [20, p. 216]. In this sense, computer security is only an additional object of encroachment, whereas the constitutional rights of an individual in the information sphere should be recognized as the main one. In the doctrine, many authors criticize the legislative decision on locating the corpus delicti in Chapter 28, and not in Chapter 19 of the CC RF [20, p. 216, 21. P.124]. However, other experts consider it expedient [22. P. 154]. In our opinion, this issue is theoretical in nature and will not have a strong impact on the law enforcement process. At the same time, we believe that personal data as information about a person cannot be separated from the personality; therefore, it would be more appropriate to place responsibility for the illegal trafficking of personal data in Chapter 19 of the CC RF. In addition, it does not seem entirely correct to introduce a special criminal law ban only because the scope of crime was turned into a virtual analogue of a

⁷ Federal Law No. 421-FZ of November 30, 2024 "On Amendments to the Criminal Code of the Russian Federation". Collection of legislation of the Russian Federation. 2024. No. 49 (part IV). Art. 7412.

physical scope; even before responsibility for the illegal trafficking of personal data (Art. 272¹ of the CC RF) was established, criminal law allowed bringing to justice persons for committing such acts.

The scope of crime according to Article 272¹ of the CC RF forms a set of three interrelated components: firstly, it is computer information; secondly, it must contain personal data; thirdly, this information must be obtained illegally. It should be pointed out that such a construction of the crime scope, combining features of a computer-technical and information-legal nature, is to a certain extent unique to the system of Russian criminal legislation and requires careful doctrinal comprehension. Should we expect, for example, the introduction of a criminal law norm for the illegal trafficking of computer information containing commercial or state secrets? Documented personal data is not protected by Article 272¹ of the CC RF; responsibility for encroachments on them is provided by the earlier criminal law norms (Article 137 of the CC RF).

From a practical point of view, the question of whether publicly available personal information can be the scope of crime under Article 272¹ of the CC RF is essential. It seems that in the presence of other signs of the crime composition, the answer should be positive: the fact that personal data is publicly available does not remove the question of the legality of their initial receipt and subsequent turnover, since Law No. 152-FZ allows the processing of publicly available personal data only for certain purposes and within the limits of their initial disclosure.

The objective side of crimes under Article 272¹ of the CC RF is a set of alternative actions with the scope of crime: illegal use, transfer (distribution, provision, access), collection and storage of computer information containing personal data. All these deeds, according to the

legal definition, relate to the types of personal data processing (Article 3 of Law No. 152-FZ). Thus, the legislator criminalizes certain forms of personal data processing, provided that the data was originally obtained illegally.

We consider it necessary to clarify the content of the concept of “illegally obtained” personal data, since this feature is systemically important for the qualification of a deed. Obtaining personal data is considered legitimate in the following cases: the consent of the personal data subject, duly executed in accordance with Article 9 of Law No. 152-FZ; cases directly provided for by law (for example, to ensure justice, to exercise state powers, to protect life or health); data received by a duly authorized person within their competence. Accordingly, obtaining personal data illegally covers all situations in which the listed conditions are not met: unauthorized access to information systems, obtaining data through deception or coercion, exceeding the limits of the subject’s consent, and other similar actions.

The problem is a situation in which the illegal trafficking of personal data is carried out by a legally functioning organization. In other words, the entity processing personal data uses them outside of the purposes established by law or contract (that is, it received them legally and uses them not only for the intended purposes, but also, for example, transfers them to third parties). It seems that in cases of illegal use or dissemination of this data, the application of Article 272¹ of the CC RF is impossible.

However, employees who sell official databases with personal information of clients may be subjects of a crime, since they could obtain such information while violating the procedure established by regulatory legal acts, regardless of the form of such access. In the disposition of the criminal law norm stipulated by Article 272¹ of the CC RF, the “illegal origin” of computer information as a sign of the crime scope

may be due to a violation of the organization's local legal acts in the field of information (digital) security, which regulate access to such information, including the purpose of such access. Violation of the relevant provisions indicates the unlawful receipt of personal data stored in the organization's information system. Accordingly, all possible subsequent deeds (use, distribution, etc.) contain elements of a crime under Article 272¹ of the CC RF. For example, from February to July 2025, a police officer, using her official position and access to a special software reserve, illegally collected and transferred monetary data about residents of Levokumsky district of Stavropol Territory. A criminal case was opened against her on the grounds of corpus delicti provided for in clause d of Part 3 of Article 272¹ of the CC RF; the investigation continues⁸.

4. Problems of qualification

A significant problem is the qualification of crimes under Article 272¹ of the CC RF in combination with related elements. For example, if illegal trafficking of personal data precedes fraudulent actions, the deed should be qualified under Articles 159 and 272¹ of the CC RF.

At the same time, it is necessary to take into account possible competition with Articles 137, 183, and 272 of the CC RF, when general rules for overcoming competition of norms should be applied: the priority of a special norm over a general one and norms in the competition of parts and the whole. Since Article 272¹ is special in relation to Article 272 of the CC RF regarding deeds with personal data and to Article 137 of the CC RF regarding computer

processing of information, the qualification of the deed according to the totality of these norms in most cases seems superfluous. In turn, attacks on personal data in an analog form entail the application of "traditional" criminal law prohibitions.

Unlawful collection of personal data should be qualified as a set of crimes provided for in Articles 272¹ and 274¹ of the CC RF, if committed by breaking the means of software and hardware protection (hacking) – a computer attack on significant objects of the critical information infrastructure of the Russian Federation. Attackers can obtain significant amounts of personal data through unlawful impact on information systems in the field of education and healthcare. For example, an employee of a telecommunication company in Magadan region, using his official position out of personal interest, committed unlawful access to legally protected computer information, thereby damaging the critical information infrastructure of Russia, and also illegally collected and distributed computer information containing personal data of citizens using the services of the said telecommunication company. He was found guilty of committing crimes stipulated in clause d of Part 3 of Article 272¹ and Part 4 of Article 274¹ of the CC RF⁹.

In Article 272 of the CC RF, the legislator made a reservation, the essence of which is to eliminate possible competition. However, unlike Article 272¹ of the CC RF, the corpus delicti provided for in Article 272 of the CC RF is formulated as material and the deed is recognized as completed at the time of the onset of socially dangerous consequences (copying, blocking,

⁸ In Levokumsky district, a police officer is suspected of illegally collecting and transferring personal data. URL: <https://stavropol.sledcom.ru/news/item/2011677/> (access date: 12.01.2026)

⁹ A communications company employee in Magadan was caught on personal data leakage. URL: <https://magadanmedia.ru/news/2418504/> (access date: 12.01.2026)

destruction, modification). Therefore, if a person unlawfully accessed the information-telecommunication infrastructure of an organization, copied computer information containing personal data, and also modified or blocked computer information by changing the access identifiers of the resource administrator or otherwise, then the deed must be qualified according to the totality of crimes provided for in Articles 272 and 272¹ of the CC RF. However, if a person only copied computer information containing personal data, they actually collected them within the meaning of Article 272¹ of the CC RF; in this case, additional qualification under Article 272 of the CC RF is not required.

Comments to Article 272¹ of the CC RF state that it does not apply to cases of processing personal data by individuals solely for personal and family needs. Hence, E.A. Ruskevich believes that the legislator formulates a kind of “universal criterion of insignificance” in order to exclude from the sphere of criminal repression certain forms of “domestic” dissemination of personal data of relatives, friends, and acquaintances, when a person does not bother to request the consent of the personal data subject [14. pp. 57–58]. It seems that this is because these deeds do not have the degree of public danger sufficient to bring a person to criminal responsibility and are clearly not related to the mass commercial “exploitation” of personal data, which is of a retaliatory nature.

5. Prospects for improving the Russian legislation

Based on the conducted research, it is possible to formulate the following proposals for improving the Russian legislation in the field of countering illicit trafficking of personal data in the data economy:

first, it is necessary to transform the disposition of the criminal law norm enshrined in Article 272¹ of the CC RF, in terms of clarifying the concept of “illegal receipt” of personal data

by introducing a reference to the grounds established by Law No. 152-FZ. Such a solution will eliminate legal uncertainty and ensure the systemic unity of criminal law and information legislation;

second, we propose adding a note to Article 272¹ of the CC RF with a condition on the exemption from criminal liability of persons who voluntarily reported the arrays of illegally obtained personal data, by analogy with the incentive norms provided for in other sections of the CC RF. This measure will expand the range of sources of information about leaks and facilitate the early detection of personal data illegal trafficking.

6. Conclusions

The conducted research allows formulating the following conclusions. The legal aspects of personal data protection are becoming increasingly relevant [23. pp. 1031–1053, 24. pp. 912–925] and need further research. The formation of the data economy has predetermined a qualitative increase in the public danger of deeds related to the illegal trafficking of personal data: being the most valuable economic resource, personal information of citizens has become a coveted object of criminal attacks, the scale and sophistication of which are constantly increasing. Introduction of Article 272¹ of the Russian Criminal Code marks a qualitatively new stage in the development of the Russian system of personal data criminal law protection. For the first time, a special criminal law instrument was created to counter this phenomenon.

At the same time, the analysis of the new norm revealed a number of problems that require legislative resolution: the inaccurate the conceptual framework, the unclear distinguishing between legitimate and illegal trafficking of personal data, and competition with related crimes.

Thus, the adopted law should be considered as an important, but not the

final step towards creating a comprehensive and effective mechanism for the criminal protection of personal data in a data economy. Further improvement of this mechanism requires consolidation of efforts of the legislator, law enforcement, and the scientific community. Therefore, research in the field of overcoming illegal cross-border transfer of personal data are also important [25. pp. 963–964].

REFERENCES

1. Afanasev S.D., Chikhladze L.T. Legal regulation of big data: modern problems in the context of the formation of the data economy. *Zakon i pravo = Law & Legislation*, 2024, no. 2, pp. 37–42. DOI: 10.24412/2073-3313-2024-2-37-42. (In Russ.).
2. Begishev I.R., Kirpichnikov D.V. Problems of personal data protection in criminal law. *Ugolovnaya yustitsiya = Russian Journal of Criminal Law*, 2020, no. 15, pp. 11–16. DOI: 10.17223/23088451/15/3. (In Russ.).
3. Shutova A.A. Social conditionality rules on the existence of criminal liability for the infringement of personal data. *Yuridicheskaya nauka i praktika: Vestnik Nizhegorodskoi akademii MVD Rossii = Legal science and practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 2015, no. 4 (32), pp. 332–335. (In Russ.).
4. Prosvetova O.B. *Personal data protection*, Cand. Diss. Thesis. Voronezh, 2005. 22 p. (In Russ.).
5. Belgorodtseva N.G. *Theoretical and legal aspects of personal data protection*, Cand. Diss. Thesis. Moscow, 2012. 25 p. (In Russ.).
6. Khokhlova E.V. *Illegal actions with personal data: criminal law research*, Cand. Diss. Belgorod, 2024. 255 p. (In Russ.).
7. Akinina N.Yu., Anisimov V.F., Kochupalov R.V. Criminalization of personal data illegal trade. *Vestnik Surgutskogo gosudarstvennogo universiteta = Surgut State University Journal*, 2024, vol. 12, no. 3, pp. 84–91. DOI: 10.35266/2949-3455-2024-3-8. (In Russ.).
8. Shchepelkov V.F. Criminal liability for illegal personal data trafficking (Article 272.1 of the Criminal Code of the Russian Federation). *Vestnik Volgogradskoi akademii MVD Rossii = Journal of the Volgograd Academy of the Ministry of the Interior of Russia*, 2025, no. 3 (74), pp. 35–42. (In Russ.).
9. Styazhkina S.A. Issues of qualification of illegal trafficking of personal data. *Vestnik Udmurtskogo universiteta. Seriya Ekonomika i pravo = Bulletin of Udmurt University. Series Economics and Law*, 2025, vol. 35, no. 5, pp. 945–952. DOI: 10.35634/2412-9593-2025-35-5-945-952. (In Russ.).
10. Esakov G.A. Illegal circulation of personal data (Art. 272.1 of the Criminal code of the Russian Federation). *Ugolovnoe pravo*, 2025, no. 11 (183), pp. 10–17. (In Russ.).
11. Chukreev V.A. Personal biometric data as subjects of criminal law protection. *Vestnik Universiteta imeni O.E. Kutafina (MGYuA) = Courier of Kutafin Moscow State Law University (MSAL)*, 2022, no. 3, pp. 107–116. DOI: 10.17803/2311-5998.2022.91.3.107-116. (In Russ.).
12. Volkova A.V. Social conditionality of criminalization of illegal actions with computer information containing personal data. *Problemy prava = Issues of law*, 2025, no. 4 (100), pp. 86–95. (In Russ.).
13. Knyazkov A.A. Criminal law novel for violation of the legislation on personal data (Art. 272¹ of the Criminal Code of Russia): design features of the composition and qualification issues. *Vestnik Universiteta imeni O.E. Kutafina (MGYuA) = Courier of Kutafin Moscow State Law University (MSAL)*, 2025, no. 5, pp. 65–73. DOI: 10.17803/2311-5998.2025.129.5.065-073. (In Russ.).
14. Russkevich E.A. On criminal liability for illegal actions with computer information containing personal data. *Ugolovnyi protsess*, 2025, no. 7 (247), pp. 53–59. (In Russ.).
15. Alikhadzhiyeva I.S. Self-serving digital crime with personal data, in: *Problemy pravookhranitel'noi deyatel'nosti na sovremennom etape*, Proceedings of the IV All-Russian (with international participation) scientific and practical conference (Kostroma, April 24–25, 2025), Kostroma, Kostroma State University Publ., 2025, pp. 167–173. (In Russ.).
16. Alikhadzhiyeva I.S. Transforming identity crime. *Vestnik Prikamskogo sotsial'nogo instituta = Bulletin of Prikamsky Social Institute*, 2025, no. 2 (101), pp. 6–12. (In Russ.).
17. Alikhadzhiyev I.S. Private Life, Personal Secret or Personal Data: How to Interpret Information about the Person to the Law Enforcement Officer?. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Istoriya i pravo = Proceedings of Southwest State University. Series: History and Law*, 2023, vol. 13, no. 3, pp. 90–101. DOI: 10.21869/2223-1501-2023-13-3-90-101. (In Russ.).
18. Alikhadzhiyev I.S. Private Life, Personal Secret or Personal Data: How to Interpret Information about the Person to the Law Enforcement Officer?. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Istoriya i pravo = Proceedings of Southwest State University. Series: History and Law*, 2024, vol. 14, no. 2, pp. 91–106. DOI: 10.21869/2223-1501-2024-14-2-91-106. (In Russ.).

19. Phuoc Thinh Tran, Khanh Truong Duong, Staroverova O.V., Leonova O.A. Data economy: barriers, problems, and solutions. *Ekonomika i upravlenie: problemy, resheniya*, 2025, no. 5 (158), vol. 9, pp. 142–155. DOI: 10.36871/ek.up.p.r.2025.05.09.017. (In Russ.).

20. Alikhajieva I.S. Bill № 502113-8 «On amending the Criminal Code of the Russian Federation (in the part of establishing responsibility for illegal use and transfer, collection and storage of computer information containing personal data)»: scientific comment. *Ugolovnoe pravo: strategiya razvitiya v XXI veke*, 2024, no. 2, pp. 213–222. (In Russ.).

21. Shutova A.A. Novelties in Russian criminal law on liability for personal data breaches. *Uchenye zapiski Kazanskogo universiteta. Seriya Gumanitarnye nauki = Kazan Journal of Historical, Linguistic, and Legal Research*, 2024, vol. 166, no. 6, pp. 122–134. DOI: 10.26907/2541-7738.2024.6.122-134. (In Russ.).

22. Shkhagapsoev Z.L. On the issue of criminal liability for illegal actions with computer information containing personal data. *Yuridicheskii vestnik Dagestanskogo gosudarstvennogo universiteta = Law herald of Dagestan State University*, 2025, vol. 54, no. 2, pp. 150–155. DOI: 10.21779/2224-0241-2025-54-2-150-155. (In Russ.).

INFORMATION ABOUT AUTHORS

Albina A. Shutova – PhD in Law; Senior Researcher, Institute of Digital Technologies and Law; Associate Professor, Department of Criminal Law and Procedure
Kazan Innovative University named after V.G. Timiryasov
42, Moskovskaya ul., Kazan, 420111, Russia
E-mail: shutova1993@inbox.ru
RSCI SPIN-code: 5235-4319; AuthorID: 835100

Ildar R. Begishev – Doctor of Law, Associate Professor, Honored Lawyer of the Republic of Tatarstan; Chief Researcher, Institute of Digital Technologies and Law; Professor, Department of Criminal Law and Procedure
Kazan Innovative University named after V.G. Timiryasov
42, Moskovskaya ul., Kazan, 420111, Russia
E-mail: begishev@mail.ru
RSCI SPIN-code: 8859-9395; AuthorID: 595003

Anna V. Volkova – applicant for PhD in Law, Department of Criminal Law and Procedure
Kazan Innovative University named after V.G. Timiryasov
42, Moskovskaya ul., Kazan, 420111, Russia
E-mail: avmail555@gmail.com

BIBLIOGRAPHIC DESCRIPTION

Shutova A.A., Begishev I.R., Volkova A.V. Criminal law protection of personal data in a data economy. *Pravoprimenenie = Law Enforcement Review*, 2026, vol. 10, no. 2, pp. 127–136. DOI: 10.52468/2542-1514.2026.10(2).127-136. (In Russ.).