IRSHAD
Uzbek Journal of Law and Digital Policy |
Volume: 3, Issue: 1
2025

Legal Protection of Personal Data in Big Data Analysis: Threats and General Rules

Mamanazarov Sardor Shukhratovich
Tashkent State University of Law

Abstract

This article provides a comprehensive analysis of the pressing issues related to personal data protection in the context of Big Data. The distinctive features of four types of data within the Big Data framework provided, observed, derived, and inferred dataalong with their protection mechanisms and security requirements are examined in detail. The principles of data protection, particularly the principles of fairness and transparency, and the necessity of implementing them in national legislation are substantiated from both theoretical and practical perspectives. The concept of threats to the security of data within the Big Data framework is developed, along with recommendations for what it should entail. The discriminatory characteristics of automated decision-making and profiling processes, as well as their impact on individual rights, are deeply analyzed. The complexity of Big Data analysis, which can lead to opacity in processing for citizens and consumers whose data is used, is highlighted. The necessity of developing new legal mechanisms to protect the rights of data subjects and ensure data confidentiality and security is substantiated.

Keywords: Big Data, Personal Data, Data Protection, Fairness Principle, Transparency Principle, Data Security, Confidentiality, Data Owner

APA Citation:

Mamanazarov, S. (2025). Legal Protection of Personal Data in Big Data Analysis: Threats and General Rules. *Uzbek Journal of Law and Digital Policy, 3*(1), 182–192. https://doi.org/10.59022/ujldp.299

I. Introduction

In the context of the rapid development of digital technologies and the sharp increase in data volume, the issue of personal data protection is becoming increasingly relevant. Big Data technologies are expanding the possibilities for collecting, processing, and analyzing personal data. This, in turn, necessitates the development of new legal mechanisms to protect the rights of data subjects and ensure data confidentiality and security. Big Data is becoming a part of regular business for many organizations in both the public and private sectors. This is due to the continuous growth of data, including data from new sources such as IoT, the development of tools for managing and analyzing this data, and the growing benefits and opportunities for entrepreneurs.

The relevance of this research lies in the fact that today Big Data technologies are widely used in public administration, commercial activities, and social spheres. According to World Bank data, global data volume is expected to reach 175 zettabytes by 2025. A large portion of this data includes personal information. Big Data is what companies use and it determines what businesses they enter (Qazi & Sher, 2016). According to the researcher, "Big Data is not only a technological development but also a socio-legal phenomenon that affects human rights and freedoms" (Mantelero, 2018).

Another important aspect determining the relevance of the topic is that problems related to personal data protection often arise due to the actions of the data subjects themselves. They place their personal information on public resources, which ultimately forms an individual's digital profile. According to a global survey by KPMG, an average of 54% of respondents expressed "concern" about how companies use their personal data. The main goal of the research is to determine the role of personal data protection principles in Big Data analysis, improve existing legal mechanisms, and develop new legal tools. To achieve this goal, the following tasks have been defined:

- Study the classification of data within Big Data;
- Analyze the basic principles of data protection;
- Identify threats to personal data security;
- Study international experience in data protection.

Several scholars have contributed to the research on this topic. One study examined the legal nature of user agreements, while another proposed using a service model within the Big Data framework (Poduzova, 2023). Some research has highlighted the consumer character of the relationships under study, while other work has explored cases of algorithmic discrimination in online advertising (Alizadeh & Nazapour Kashani, 2023). Analysis of foreign regulatory approaches shows that various aspects of data protection in Big Data analysis are addressed in legal frameworks such as the General Data Protection Regulation of the European Union, the Fair Credit Reporting Act of the

United States, the Personal Information Protection Act of Japan, and the Personal Data Protection Act of South Korea (Revillod, 2024).

II. Methodology

During the research process, a comprehensive methodological approach was applied to determine the role of data protection principles in Big Data analysis. The study of the formation and development stages of the personal data protection institution and the analysis of the evolution of legal regulation of Big Data technologies. Through this method, the history of the formation of the Law of the Republic of Uzbekistan "On Personal Data" (Law of the Republic of Uzbekistan, 2019), GDPR (General Data Protection Regulation, 2016), and other legal documents was studied, revealing the development trends of data protection principles.

The comparative-legal method was applied to analyze data protection mechanisms within the Big Data framework across various jurisdictions, including the United States, the European Union, Japan, South Korea, and Singapore. This approach facilitated the examination of advanced foreign practices and the development of recommendations for improving national legislation. Using this method, key legal frameworks such as the Federal Trade Commission’s "Fair Information Practice Principles" and Japan’s Privacy Law, as outlined by the Japanese Personal Information Protection Commission in 2023, were analyzed to understand different regulatory approaches.

The systematic-structural method played a crucial role in classifying data within the Big Data framework, organizing data protection principles, and identifying the interconnections among them. Through this method, distinctions between four types of data provided, observed, derived, and inferred were systematically identified, highlighting their unique characteristics and regulatory implications. The statistical analysis method was employed to assess and summarize research findings from international organizations such as KPMG International and the Boston Consulting Group in 2023, along with statistics on database usage. This method provided insight into global trends and challenges in personal data protection, offering a data-driven perspective on emerging risks and regulatory gaps.

The sociological research method enabled an exploration of public attitudes toward personal data privacy and security. A survey conducted among more than 200 respondents in Uzbekistan revealed critical insights into data protection awareness and behavior. The results indicated that 20% of respondents do not take measures to keep their personal data confidential, while 50% expressed trust in internet sites regarding their personal information. The following materials were used as research sources:

- International legal documents (GDPR and others);

- National legislative documents;
- Judicial practice materials;
- Reports from international organizations;
- Scientific literature;
- Statistical data;
- Survey results.

The research object selected was social relations related to personal data protection in Big Data analysis. The subject consisted of the system of legal norms and mechanisms regulating these relations.

III. Results

A. Data Classification in Big Data Analysis and Security Threats

According to the research results, four types of data are distinguished within the Big Data framework:

1. Provided data - data consciously given by individuals. For example:
   - Data provided through filling out online forms
   - Information entered during registration on social networks
   - Answers entered in questionnaires and surveys
2. Observed data - data recorded automatically:
   - Data collected through online cookies
   - Data recorded using sensors
   - Data obtained through facial recognition cameras
   - Data from IoT devices
3. Derived data - data that is relatively simply and directly produced from other data. For example:
   - Calculating customer profitability
   - Analysis of user purchasing habits
   - Calculating a reliability indicator based on a customer's payment history
1. Inferred data - data produced using complex methods of analysis by finding correlations between data sets and using them to categorize or profile people:
   - Calculating credit scores
   - Predicting the likelihood of future purchases
   - Predicting future health outcomes

As a research result, the concept of threats to personal data security was developed and reflected in clause 7, first paragraph, of the regulation approved by Resolution No. 570 of the Cabinet of Ministers of the Republic of Uzbekistan dated October 5, 2022 (Resolution No. 570, 2022). According to it, threats to personal data security are a

combination of conditions and factors that may lead to unauthorized, including accidental, access to the database resulting in modification, addition, use, transfer, distribution, transmission, depersonalization, destruction, copying, and other illegal actions with personal data.

The results of a global survey by KPMG (KPMG International, 2023) showed that an average of 56% of respondents expressed "concern" about how companies use their personal data. Boston Consulting Group studies (Boston Consulting Group, 2023) indicate that for 75% of consumers in most countries, the privacy of their personal data remains the most important issue.

The results of the conducted sociological survey showed that 20% of respondents reported not keeping their personal data confidential. Furthermore, to the question "What do you do to ensure privacy and security of personal data on the Internet?" in the survey, 50% of participants answered, "I trust internet sites, there is no need to think about security." This, in turn, indicates the need to raise the legal culture of the population.

B. Improving Data Protection Principles and Legal Mechanisms

According to the research results, the essential basic principles in the processing process within the Big Data framework consist of the following:

1. Fairness principle

The need to reflect in national legislation the requirement stated in GDPR Article 5(1)(a) that data must be processed fairly, lawfully, and transparently in relation to the data subject was identified. This principle is fundamental to ensuring that personal data processing respects individual rights and promotes accountability among data controllers. Various jurisdictions have incorporated this principle into their national laws to align with international standards on data protection.

In Japan, Article 6 of the Personal Information Protection Law enshrines the principle of fair and lawful data processing, ensuring that personal data is handled with due regard for the rights and interests of individuals. Similarly, Article 5 of the Federal Law of the Russian Federation stipulates that the processing of personal data should be carried out on the basis of the principles of legality and fairness. This approach establishes a clear obligation for data controllers to process information in a manner that upholds ethical and legal standards. In the United States, the Federal Trade Commission has developed the Fair Information Practice Principles (FIPPs), which emphasize fairness, transparency, and accountability in data processing activities.

However, an analysis of the Law of the Republic of Uzbekistan "On Personal Data" (2019) revealed that the principle of fairness is not mentioned once throughout the entire text of the law. This omission creates a gap in ensuring that data subjects' rights are adequately protected and that data controllers operate under clear ethical guidelines. To

address this issue, it was proposed to supplement Article 5 of the law with a third paragraph containing the following provision: "fairness and non-discrimination." By incorporating this principle, Uzbekistan's legal framework on personal data protection would align more closely with international best practices, enhancing trust and legal certainty in data processing activities.

2. Transparency principle

According to Article 12 of the General Data Protection Regulation (GDPR), information about the processing of personal data and related rights should be provided in a concise, transparent, understandable, and easily accessible form. This principle plays a crucial role in ensuring that data subjects are fully aware of how their personal data is being used and the potential consequences of such processing. By making information clear and accessible, individuals can make informed decisions about their data and exercise their rights effectively.

Transparency in data processing procedures is essential to building trust between data controllers and data subjects. When organizations provide clear explanations of how data is collected, stored, and processed, individuals can better understand how their personal information is handled. This openness helps prevent misuse of data and promotes compliance with legal requirements, ensuring that processing activities align with data protection principles.

Another key aspect of this principle is the clear communication of data subjects' rights. GDPR grants individuals several rights, such as the right to access, rectify, erase, and restrict the processing of their personal data. By presenting this information in an understandable manner, organizations empower individuals to take control of their data and exercise their rights without unnecessary obstacles. Effective communication of these rights strengthens data protection and enhances individuals' confidence in the digital environment.

3. Reasonable expectation principle

A new principle has been proposed for inclusion in national legislation to strengthen the legal protection of data subjects' reasonable expectations regarding the use of their data. This principle ensures the limitation of unexpected ways of using data and guarantees the rights of data subjects.

As a result of the research, in order to enhance the protection of personal data in automated decision-making and profiling processes, it has been proposed to amend Article 25 of the Law "On Personal Data" by adding part 5 with the following content: "It is prohibited to make personal decisions based solely on automated processing, including the results of profiling. This rule does not apply to cases where the decision is necessary for the execution of a contract concluded with the data subject or where the data subject

has given clear and explicit consent. It also does not apply if the decision is permitted by legislation and appropriate measures to protect the rights and freedoms of the data subject are provided for."

To further clarify and expand the conditions for processing personal data, it has been proposed to amend Article 18 of the law by adding part 4 with the following wording: "Personal data may be processed without the consent of individuals when it is necessary for state bodies and organizations to perform functions and powers assigned to them by law. Personal data may also be processed without consent when it is necessary to ensure the legitimate interests of the data processor (operator) or third parties, except in cases where the fundamental rights and freedoms of the personal data subject prevail."

IV. Discussion

A. The Importance of Fairness and Transparency Principles in Big Data Analysis

Analysis of the research results shows that with the development of Big Data technologies, the importance of personal data protection principles is increasing. The establishment of the requirement in GDPR Article 5(1)(a) (General Data Protection Regulation, 2016) that data "must be processed fairly, lawfully, and transparently in relation to the data subject," as well as the enshrinement of the principle of fair and lawful data processing in Article 6 of the Japanese law (Japanese Personal Information Protection Commission, 2023), and the provision in Article 5 of the Federal Law of the Russian Federation (Russian Federal Law, 2006) that the processing of personal data should be carried out on the basis of the principles of legality and fairness, indicates the necessity of introducing such a norm in our national legislation as well.

The "Fair Information Practice Principles" (Federal Trade Commission, 2023) developed by the US Federal Trade Commission also require organizations to ensure transparency, purpose limitation, data quality, and security in collecting and using data. The research found that among the legal requirements that must be complied with in the process of handling personal data, the most important is fairness, which serves as the main criterion for evaluating any Big Data system. It was found that discriminatory behavior in the profiling process is associated with its "opacity" characteristic. That is, there is a problem that the reasons for the decision-making process are not clear because it is carried out through complex algorithms. According to Mariko Kawaguchi's research (Kawaguchi, 2023), "Big Data algorithms used in advertising systems have discriminatory tendencies towards young people and women."

They emphasize that contracts for the use of personal data in Big Data analysis require special attention. However, we cannot fully agree with Puchkov’s consideration that these relationships have only a consumer character, as these relationships have a

multifaceted character. The results of research show that "although people express concerns about the unwelcome use of their data affecting their privacy, in practice, they still continue to transmit their data through online systems." This indicates the need for a deeper study of the "privacy paradox" problem (Durnell et al., 2020). According to research by the International Institute of Communications, "people's willingness to provide personal data and their attitude towards how this data is used depends on specific situations." This indicates the need to apply a contextual approach in developing data protection mechanisms.

B. Issues of Data Security and Improvement of Legal Mechanisms

The analysis of research results shows that with the development of Big Data technologies, ensuring the security of personal data is becoming more complex. According to the conducted sociological survey, 20% of respondents stated that they do not keep their personal data confidential, and 50% of participants trust internet sites, which indicates the existence of serious problems in this area. The results of the global survey by KPMG (KPMG International, 2023) (56% of respondents being concerned) and Boston Consulting Group studies (Boston Consulting Group, 2023) (privacy being an important issue for 75%) differ significantly from the results of our survey. This difference is explained by the following factors:

- Characteristics of national mentality
- Level of information technology development
- Level of legal culture
- Awareness about data protection

We approve the results of the Annenberg School of Communication's study on American consumers (Annenberg School for Communication, 2023). It criticized the idea that consumers continue to provide their data to marketers because they consciously participate in the process of exchanging personal data for benefits such as discounts. Instead, the study concluded that "most Americans think it's futile to try to control what companies learn about them."

During the research, we concluded that it is necessary to implement in our national legislation the GDPR's (General Data Protection Regulation, 2016) requirement that information about the personal data processing process and related rights should be provided in a "concise, transparent, understandable, and easily accessible form." Also, based on the experience of Japan (Japanese Personal Information Protection Commission, 2023) and Singapore (Personal Data Protection Act, 2021), it is proposed to include in our national legislation the requirement that companies publish and fully explain to users a detailed privacy policy on how personal data is used.

It was found that the complexity of Big Data analysis, including the application of

artificial intelligence and machine learning approaches, can serve as a factor that makes it difficult for organizations to ensure transparency in personal data processing processes. On this issue, we approve the approach of scientists (Sato, 2023) that enterprises using Big Data technologies must comply with all legal requirements ensuring data protection and privacy in processes related to people's personal data.

To address these challenges, it is essential to align national legislation with international standards, ensuring that legal frameworks effectively regulate emerging issues in the digital space. Enhancing public awareness and legal literacy among data subjects is crucial for fostering a culture of compliance and responsible digital behavior. Strengthening technical and organizational measures for data protection will help safeguard sensitive information and mitigate cyber risks. Establishing more effective control mechanisms can enhance regulatory oversight and enforcement, ensuring accountability in digital interactions. Furthermore, fostering international cooperation is vital for addressing cross-border cyber threats, harmonizing legal approaches, and facilitating the exchange of best practices in cybersecurity and digital governance

Conclusion

There are four types of data within the Big Data framework provided, observed, derived, and inferred data each requiring its own protection mechanisms. It was found that such a classification of data does not exist in national legislation. Therefore, it is proposed to introduce a classification of data into the Law of the Republic of Uzbekistan "On Personal Data". The concept of threats to personal data security was developed and reflected in the regulation approved by Resolution No. 570 of the Cabinet of Ministers of the Republic of Uzbekistan dated October 5, 2022. This concept covers modification, addition, use, transfer, distribution, transmission, depersonalization, destruction, copying, and other illegal actions with personal data as a result of unauthorized access to the database.

The importance of the fairness principle in the Big Data analysis process was identified. However, the fairness principle is not mentioned at all in the Law of the Republic of Uzbekistan "On Personal Data." Therefore, it is proposed to supplement Article 5 of the law with the principle of "fairness and non-discrimination. “The necessity of introducing the "reasonable expectation" principle into national legislation was substantiated. This principle allows legal protection of data subjects' reasonable expectations regarding the use of their data. To ensure the protection of personal data in automated decision-making and profiling processes, it was proposed to supplement Article 25 of the Law "On Personal Data" with a new part. This norm provides for mechanisms to protect data subjects from the effects of automated decisions.

To further clarify and expand the conditions for processing personal data, it was

proposed to introduce a new part to Article 18 of the law, providing for the possibility of processing without consent when necessary for state bodies and organizations to exercise their legal powers. The results of the conducted sociological research showed the need to raise the legal culture of the population regarding personal data protection. The fact that 50% of respondents trust internet sites and do not think about security indicates the need to conduct extensive explanatory work in this area. Based on these conclusions, the recommendations developed for improving the system of personal data protection in Big Data analysis are important for the development and practical application of national legislation. In the future, it would be expedient to continue studying international experience in this field and adapting national legislation to international standards.

Bibliography

Alizadeh, H., & Nazapour Kashani, H. (2023). An empirical study of consumer-brand relationships in the hospitality industry. *Interdisciplinary Journal of Management Studies (Formerly known as Iranian Journal of Management Studies)*, *16*(4), 857-872. https://doi.org/10.22059/ijms.2022.341453.675074

Durnell, E., Okabe-Miyamoto, K., Howell, R. T., & Zizi, M. (2020). Online privacy breaches, offline consequences: Construction and validation of the concerns with the protection of informational privacy scale. *International Journal of Human–Computer Interaction*, *36*(19), 1834–1848. https://doi.org/10.1080/10447318.2020.1794626

Mantelero, A. (2018). AI and big data: A blueprint for a human rights, social and ethical impact assessment. *Computer Law & Security Review*, *34*(4), 754-772. https://doi.org/10.1016/j.clsr.2018.05.017

Poduzova, E. B. (2023). Personal data of the patient and his legal representative: The specifics of electronic provision in the context of the use of «artificial intelligence» technologies in digital medicine. *Actual Problems of Russian Law*, *18*(4), 86–92. https://doi.org/10.17803/1994-1471.2023.149.4.086-092

Qazi, R. U. R., & Sher, A. (2016). *Title of the article*. The International Technology Management Review, 6(2), 50–63. https://doi.org/10.2991/itmr.2016.6.2.3

Revillod, G. (2024). Why do Swiss HR departments dislike algorithms in their recruitment process? An empirical analysis. *Administrative Sciences*, *14*(10), 253. https://doi.org/10.3390/admsci14100253