World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-63 October-2026
ISSN: 2749-3601

ISSUES OF PROTECTING CITIZENS' PERSONAL NON-PROPERTY RIGHTS IN THE USE OF GEOGRAPHIC INFORMATION SYSTEMS

Zafar Babakulov
Doctor of Science in Law (DSc), Associate Professor
Email: zafarbabakulov11@gmail.com

Article history:

Received: 11th August 2026
Accepted: 10th September 2026

Abstract:

This article was prepared within the framework of the applied scientific research project entitled "Development of Software for a Geoinformation Map of Tashkent City for Monitoring the Criminogenic Situation," implemented under **State Research Contract No. AL-11325078166.** The article examines civil-law mechanisms for protecting citizens' personal non-property rights in the use of geographic information systems, including the rights to privacy, personal data protection, honor, dignity, and other intangible interests. Based on a comparative analysis of the legislation of the European Union, the United States, the United Kingdom, and China, as well as scholarly perspectives, the study explores legal challenges related to geolocation data processing, re-identification, digital surveillance, and unlawful disclosure of personal information. The research develops scientific and practical proposals aimed at improving preventive, restorative, and compensatory civil-law mechanisms for protecting personal non-property rights in geographic information systems.

Keywords: geographic information systems, personal non-property rights, right to privacy, geolocation, geoprivacy, personal data, re-identification, restoration of rights, non-pecuniary damage, civil liability.

INTRODUCTION.

The development of geoinformation technologies has expanded opportunities for the use of spatial data in public administration, public safety, urban planning, transportation, healthcare, and other sectors. These technologies enable the analysis of geographical distributions of objects, population movements, social processes, and various events within specific areas. However, the processing of citizens' residential addresses, movement histories, location records, and information about their personal activities through geographic information systems may pose risks to their personal non-property rights.

Unlike conventional information systems, geographic information systems process data in relation to specific locations and time periods. Consequently, information that does not directly identify an individual may enable their identification when combined with other datasets. Therefore, the legal protection of geospatial data extends beyond information security. It also encompasses civil-law safeguards aimed at preventing unjustified interference with private life, restricting data processing to lawful purposes, correcting inaccurate information, and restoring violated rights.

Huan Li, Jianwei Huang, and Mei-Po Kwan argue that the protection of geospatial data is closely connected not only with technical measures but also with legal regulation, social relations, and citizens' attitudes toward privacy [1, pp. 1–2].

RELEVANCE OF THE RESEARCH TOPIC.

The increasing use of geographic information systems has intensified the need to establish clear legal boundaries for protecting individuals' location data and movement histories. In particular, the integration of different databases and their analysis using artificial intelligence create risks of re-identification, disclosure of private information, and unjustified digital surveillance.

According to Milad Malekzadeh, Yan Kestens, and Justine I. Blanford, the distinctive characteristics of geospatial data require specific protective measures beyond those applicable to conventional personal data. Location information may indirectly reveal an individual's movement patterns, activities, and social relationships [2, pp. 2–3]. Shelby Stender, examining geofence warrants in the United States, emphasizes that such mechanisms may enable law enforcement authorities to obtain the location histories of individuals who are not involved in criminal activities [3, pp. 733–734].

In Uzbekistan, the development of geographic information systems highlights the importance of strengthening the protection of citizens' personal non-property rights, clarifying the obligations of data controllers, and improving civil-law mechanisms for

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-63 October-2026
ISSN: 2749-3601

compensating damage caused by the unlawful use of geospatial data.

RESEARCH METHODS.

The study employed formal legal, comparative legal, systemic and structural, logical analysis, critical evaluation of scholarly perspectives, and legal modeling methods. The formal legal and comparative legal methods were used to examine the legal frameworks governing the protection of geospatial data and personal non-property rights in the European Union, the United States, the United Kingdom, China, and Uzbekistan. Systemic and critical analysis methods were applied to evaluate foreign scholars' perspectives on geoprivacy, re-identification, and digital surveillance. Legal modeling was used to develop proposals for improving mechanisms for restoring violated rights and establishing civil liability in the use of geographic information systems.

Research Results.

When examining the protection of personal non-property rights in geographic information systems (GIS), it is essential to determine the legal nature of geospatial data. Not all information processed through GIS constitutes personal data. For example, information concerning transport infrastructure, environmental conditions, or aggregated demographic indicators does not qualify as personal data if it does not allow an individual to be identified. However, combining such information with residential addresses, movement histories, or other datasets may enable the identification of a natural person.

Huan Li, Jianwei Huang, and Mei-Po Kwan argue that geoprivacy protection cannot be limited to technical security measures. Their study analyzed 526 scientific publications from 2008–2024 and surveyed 4,260 respondents in Hong Kong, Japan, New Zealand, South Korea, the United Kingdom, and the United States. The findings demonstrate that attitudes toward geoprivacy protection are influenced by cultural characteristics, regulatory frameworks, and public perceptions of privacy [1, pp. 1–2].

Milad Malekzadeh, Yan Kestens, Justine I. Blanford, and their co-authors distinguish three categories of geospatial data: static location data, dynamic data reflecting individuals' movements, and derived geographic data inferred from other information [2, pp. 3–4]. This classification is legally significant because a single record of an individual's residential address and a detailed history of their movements may involve different levels of interference with private life.

Two principal characteristics of geospatial data should be considered when assessing their relationship with personal non-property rights. First, such data may contain information about an individual's private life. Second, their processing or disclosure may adversely affect other intangible interests. Article 99 of the Civil Code of the Republic of Uzbekistan recognizes honor, dignity, personal inviolability, personal and family secrets, privacy, and other intangible benefits as objects of civil-law protection [3].

Accordingly, the unlawful disclosure of an individual's residential address or movement history through a geographic information system may constitute an infringement of the right to privacy. Where false information damaging a person's honor, dignity, or business reputation is disseminated, the remedies provided under Article 100 of the Civil Code may also become applicable.

Nevertheless, the processing of geospatial data should not automatically be equated with an infringement of personal non-property rights. The lawful processing of location data for legitimate and necessary purposes does not in itself constitute a violation. Legal assessment must consider the grounds for data collection, the purposes of processing, necessity, the nature of disclosure, and the impact on individual rights.

In our view, the distinctive nature of civil-law protection in geographic information systems lies not primarily in the independent economic value of geospatial data, but in its potential impact on privacy, personal freedom, and other intangible interests.

One of the principal threats to privacy in geographic information systems is the possibility of re-identifying individuals from anonymized geospatial datasets. Even where names and other direct identifiers have been removed, movement patterns and records of visits to particular locations may still enable the identification of individuals.

Malekzadeh and his co-authors emphasize that geospatial data differ from other categories of information because of their inherent spatial and temporal characteristics. In their view, even limited movement data, when combined with additional information, may reveal new details about an individual's private life [2, pp. 2–3].

The researchers propose a framework for geoprivacy protection covering five stages: data collection, storage, sharing, analysis, and dissemination of results. Their framework includes 60 guiding questions designed to assess the characteristics and granularity of geographic data, their potential linkage with other information, and the risks posed to privacy [2, pp. 1–3].

This approach also has important implications for civil law. A GIS operator may initially process information that does not directly identify a person. However, if subsequent combination with other datasets makes identification possible, the legal status of the information must be reassessed.

According to Li, Huang, and Kwan, although anonymization, encryption, and other technical safeguards are essential for protecting geospatial data,

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-63 October-2026
ISSN: 2749-3601

their implementation requires balancing data utility with the level of privacy protection [1, p. 2]. Their findings suggest that legal safeguards should address not only direct identifiers but also the possibility of indirect identification.

In our view, anonymization does not automatically remove geospatial information from the scope of personal data protection. Where re-identification remains reasonably possible, the relevant data should continue to be subject to applicable personal data protection requirements.

One of the principal legal instruments governing personal data protection in geographic information systems within the European Union is Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, known as the General Data Protection Regulation (GDPR) [4]. Article 4 defines personal data as information relating to an identified or identifiable natural person and expressly includes location data among the identifiers that may enable identification.

Under Article 5 of the GDPR, personal data processing must comply with the principles of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality. Applied to geographic information systems, these principles demonstrate that the legality of geolocation data processing depends not merely on technological capabilities but on the existence of a lawful basis, a legitimate purpose, and the necessity of the processing.

Article 6 of the GDPR establishes the legal grounds for personal data processing. Consent is not the sole lawful basis. Depending on the circumstances, processing may also be justified by contractual necessity, compliance with a legal obligation, protection of vital interests, performance of a task carried out in the public interest, or other grounds provided by the Regulation. Consequently, the lawful grounds for processing geospatial data may differ between public and private geographic information systems.

Article 17 establishes the right to request the erasure of personal data under specified conditions, while Article 25 introduces the principle of data protection by design and by default.

In the context of geographic information systems, this principle requires privacy safeguards to be incorporated into the initial design of software architecture. Such measures may include restricting access to personal data, limiting the precision of location information to what is necessary, establishing retention periods, and implementing safeguards against re-identification.

Under Article 82 of the GDPR, any person who has suffered material or non-material damage as a result of an infringement of the Regulation has the right to receive compensation. However, where personal data are processed by competent law enforcement authorities for the purposes of preventing, investigating, detecting, or prosecuting criminal offences, Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 applies under the conditions specified therein. Article 56 of the Directive also provides for the right to compensation for material and non-material damage [5].

Accordingly, the legal framework governing personal data protection in geographic information systems should be determined not merely by whether the system belongs to a public or private organization, but primarily by the specific purposes and legal grounds of data processing.

In our view, the principal significance of the European Union's experience for Uzbekistan lies in ensuring both the lawfulness of geospatial data processing and the effective exercise of individuals' rights to request the correction or erasure of their data, the cessation of unlawful processing, and compensation for damage.

In the United States, the constitutional limitations on government access to geolocation data are primarily derived from the Fourth Amendment to the United States Constitution, which protects individuals against unreasonable searches and seizures.

Geofence warrants are legal instruments used to obtain historical location information about mobile devices present within a specified geographical area during a particular period.

In his 2024 article published in *Utah Law Review*, Shelby Stender critically examines the constitutionality of such warrants under the Fourth Amendment. Stender argues that geofence warrants often fail to identify with sufficient particularity the individuals whose data are sought. According to the author, such warrants do not satisfy the constitutional requirements of probable cause and particularity [6, pp. 733–734].

Stender's analysis extends beyond the legality of obtaining personal information. He emphasizes that individuals whose geolocation data have been unjustifiably collected by government authorities may have limited opportunities to obtain effective remedies. Accordingly, the author advocates stronger legislative restrictions alongside judicial safeguards [6, pp. 733–734].

Stender's arguments raise an important theoretical issue from the perspective of civil law: the existence of constitutional safeguards against unlawful data collection does not necessarily guarantee effective civil-law remedies for affected individuals. Therefore, where personal data are unlawfully collected or disclosed through geographic information systems, individuals should have access to independent legal remedies.

Such remedies may include the cessation of unlawful data processing, erasure of information under legally prescribed conditions, restrictions on further disclosure, and compensation for damage.

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-63 October-2026
ISSN: 2749-3601

When assessing the civil-law implications of the United States' experience, it is necessary to distinguish constitutional violations from tort liability. A finding that the collection of information violates constitutional requirements does not automatically establish an obligation to compensate for damage. A civil claim must have an independent legal basis and satisfy the applicable conditions for liability.

In our view, Uzbekistan's legal framework governing geographic information systems should clearly define the purposes of geolocation data collection, its geographical and temporal limits, and the authority to access such information. Judicial oversight of the lawfulness of data processing and effective mechanisms for restoring violated personal non-property rights should also be ensured.

In the United Kingdom, the civil-law protection of geospatial data is closely connected with personal data protection legislation. Section 169 of the Data Protection Act 2018 establishes the right of individuals who suffer damage as a result of infringements of applicable data protection legislation to claim compensation from data controllers or, under specified conditions, data processors [7].

An important feature of this provision is the distinction between the liability of data controllers and data processors. A controller may be held liable for damage resulting from processing that infringes the applicable legal requirements. A processor may incur liability where it breaches legal obligations specifically imposed upon processors or acts outside or contrary to the controller's lawful instructions.

Furthermore, Section 169(5) of the Act recognizes that damage includes not only financial loss but also non-material harm, such as distress.

This provision is particularly significant for protecting personal data in geographic information systems. The unlawful disclosure of geolocation information may interfere with an individual's private life and cause non-material harm even where no financial loss has occurred.

The Personal Information Protection Law of the People's Republic of China, adopted in 2021, also provides an important legal framework for personal data protection. Article 28 identifies location and movement-tracking information among categories of sensitive personal information requiring enhanced protection under the conditions established by law [8].

This approach recognizes that geospatial information may have a particularly significant impact on an individual's private life. Article 69 further establishes that a personal information processor may be held civilly liable for damage caused to an individual's rights and interests through personal information processing unless the processor proves that it was not at fault.

Such an approach may help address the imbalance in access to evidence between data subjects and information system operators, since the technical circumstances of data processing are generally better known to the operator.

A comparative assessment of the United Kingdom and China reveals different emphases in their approaches to civil liability. The United Kingdom's legislation distinguishes the legal responsibilities of controllers and processors, while China's legislation places particular emphasis on protecting sensitive personal information and allocating the burden of proving fault.

In our view, certain elements of these approaches could be incorporated into Uzbekistan's legal framework to clarify the civil-law obligations of geographic information system operators, technical data processors, and software developers.

Where personal non-property rights are infringed through the use of geographic information systems, the principal objectives of civil-law protection are to terminate unlawful conduct, restore violated rights, and, where the applicable legal conditions are satisfied, compensate for the resulting damage.

Civil liability in this context may arise from the unlawful disclosure of an individual's movement history or residential address; the processing of geolocation data for purposes beyond those originally established; the dissemination of conclusions adversely affecting an individual's rights based on inaccurate information; or damage resulting from a failure to comply with data protection obligations. Nevertheless, the establishment of civil liability in each case depends on the grounds and conditions prescribed by the applicable legislation.

Article 99 of the Civil Code of the Republic of Uzbekistan establishes the general legal protection of personal non-property rights, while Article 100 provides specific remedies for the protection of honor, dignity, and business reputation [3]. Article 985 establishes the general grounds for obligations arising from damage caused to another person, whereas Articles 1021–1022 regulate the grounds for compensation for moral damage and the determination of its amount [9].

These provisions may be applied where personal non-property rights are infringed through geographic information systems. In such cases, the nature of the violation, the damage suffered, the causal relationship, and the applicable conditions of liability must be taken into account.

In addition, Article 28 of the Law of the Republic of Uzbekistan No. ZRU-547 of 2 July 2019, "On Personal Data," governs the confidentiality of personal data. Articles 30–31 establish the rights and obligations of data subjects, data owners, and operators, while Articles 32–33 regulate dispute resolution and liability for violations of personal data legislation [10].

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-63 October-2026
ISSN: 2749-3601

From the perspective of civil-law protection, these provisions are significant because they establish a legal relationship between the rights of data subjects and the obligations of entities processing their personal information.

Nevertheless, the technical characteristics of geographic information systems create additional legal challenges. In particular, processing involving multiple operators, the generation of new information through algorithmic analysis, and the possibility of re-identifying individuals from anonymized datasets may complicate the identification of the party responsible for an infringement.

Accordingly, it can be concluded that civil-law mechanisms for protecting personal non-property rights in geographic information systems should not be limited to compensation for damage, but should also encompass measures aimed at preventing violations of individual rights during data processing and ensuring the effective restoration of violated rights.

DISCUSSION.

An analysis of foreign scholarly research and legislation indicates that traditional approaches to protecting personal non-property rights in geographic information systems are evolving. While earlier approaches primarily focused on maintaining data confidentiality and preventing unauthorized access, contemporary research increasingly emphasizes re-identification risks, the social consequences of data processing, individuals' control over their personal information, and effective remedies for violations of their rights.

The first trend involves linking geospatial data protection to individuals' ability to exercise control over their personal information. Malekzadeh and his co-authors argue that geoprivacy extends beyond conventional information confidentiality. In their view, the temporal characteristics, spatial precision, and potential linkage of geospatial data with other information are essential factors in determining the extent of interference with private life [2, pp. 2–3]. This approach demonstrates the need to supplement confidentiality safeguards with mechanisms enabling individuals to exercise control over the purposes and entities involved in processing their personal information.

The second trend concerns the legal assessment of risks associated with re-identification. Li, Huang, and Kwan emphasize that anonymization and other technical measures, although essential for protecting geospatial data, must be integrated with appropriate legal and organizational safeguards [1, p. 2]. Accordingly, where anonymized data can be combined with other information to identify an individual, their legal status should be reassessed.

The third trend involves incorporating geospatial data protection requirements at the system design stage. Article 25 of Regulation (EU) 2016/679 establishes the principle of data protection by design and by default, requiring appropriate safeguards to be integrated into information systems from the outset [4]. In geographic information systems, this approach supports the implementation of access restrictions, data retention limits, processing logs, and measures aimed at reducing re-identification risks.

The fourth trend concerns strengthening legal oversight of geolocation data processing. Stender's research demonstrates that geofence warrants may encompass location information relating not only to individuals suspected of criminal activity but also to numerous uninvolved citizens [6, pp. 733–734]. This finding highlights the importance of establishing clear legal grounds and limitations for government access to geolocation data.

The fifth trend involves improving compensation mechanisms for violations of personal non-property rights. In its judgment of 20 June 2024 in *AT and BT v PS GbR and Others* (Case C-590/22), the Court of Justice of the European Union recognized that a loss of control over personal data may, under certain circumstances, constitute non-material damage. However, a successful compensation claim requires proof of actual damage and a causal relationship between the infringement and the damage suffered [11]. This judicial approach is relevant to assessing compensation for non-material harm resulting from the unlawful disclosure of residential addresses, movement histories, or other private information through geographic information systems.

In Uzbekistan, the legal framework for protecting personal non-property rights in geographic information systems is established by the Civil Code, the Law "On Personal Data," and other regulatory legal acts.

In this regard, Resolution No. 21 of the Plenum of the Supreme Court of the Republic of Uzbekistan dated 24 November 2025, "On Judicial Practice in the Application of Legislation on the Protection of Personal Non-Property Rights and Other Intangible Benefits," is particularly significant [12]. Paragraph 1 of the Resolution recognizes the protection of personal data and the rights to request the correction of inaccurate information and the deletion of information unlawfully collected or no longer supported by a lawful basis. The Resolution also identifies privacy, personal data protection, honor, dignity, and other personal non-property rights as interests subject to judicial protection.

These clarifications are particularly relevant where citizens' personal information is unlawfully collected, disclosed, or processed for purposes beyond those originally established through geographic information

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-63 October-2026
ISSN: 2749-3601

systems. For example, where a person's residential address, movement history, or other personal information is unlawfully disclosed on a geospatial map, the affected individual may, subject to the applicable legal requirements, seek erasure of the information, cessation of unlawful processing, and restoration of violated rights.

Furthermore, paragraphs 15–17 of the Resolution emphasize the need to distinguish claims concerning the protection of honor, dignity, and business reputation from claims involving other personal non-property rights. This distinction is important because the unlawful disclosure of accurate information through a geographic information system may independently constitute an infringement of privacy.

In our view, the Resolution provides an important foundation for applying existing national legislation to the protection of personal non-property rights in geographic information systems. Nevertheless, certain issues require further legal clarification, particularly the distinctive characteristics of geolocation data, re-identification risks, processing involving multiple operators, and the assessment of damage resulting from automated analysis.

Based on the analysis of foreign research, legislation, and national judicial practice, the following proposals are advanced to strengthen the protection of citizens' personal non-property rights in geographic information systems.

First, it is proposed to supplement the Law of the Republic of Uzbekistan No. ZRU-547 of 2 July 2019, "On Personal Data," with a provision establishing specific safeguards for processing information concerning individuals' locations and movement histories. Such a provision should define lawful processing purposes, necessity and proportionality requirements, retention periods, access authorization, and obligations to assess re-identification risks.

Second, it is proposed to establish a legal obligation to incorporate personal data protection requirements into the design of geographic information systems as a preventive civil-law safeguard. These requirements should include anonymization, access restrictions, processing logs, and mechanisms for monitoring compliance with the established purposes of data processing.

Third, it is proposed to establish a specific procedure enabling data subjects to exercise their rights to verify, correct, erase, or restrict the processing of inaccurate location data or unfounded conclusions derived from such data where their personal non-property rights have been infringed, subject to the conditions prescribed by law.

Fourth, it is proposed to clarify the civil-law obligations of geographic information system operators, software developers, and technical data processors. Responsibility for determining the purposes and means of processing, maintaining data security, ensuring accuracy, and remedying infringements should be allocated according to the respective legal duties of the parties involved.

Fifth, it is recommended to review and systematize judicial practice concerning the application of Resolution No. 21 of the Plenum of the Supreme Court of the Republic of Uzbekistan dated 24 November 2025 to disputes arising from the use of geographic information systems. Particular attention should be given to the unlawful disclosure of geolocation data, re-identification, loss of control over personal information, and criteria for assessing compensation for moral damage.

Sixth, it is proposed that contracts relating to geographic information systems developed under government-funded projects expressly define obligations concerning personal data protection, confidentiality, data integrity, notification of security incidents, timely correction of inaccurate information, and compensation for damage resulting from contractual breaches or other unlawful conduct.

These proposals are intended to promote the integrated development of preventive, restorative, and compensatory civil-law mechanisms for protecting personal non-property rights in geographic information systems.

CONCLUSION

The analysis of foreign scholarly research, legislation, and judicial practice concerning the protection of citizens' personal non-property rights in the use of geographic information systems leads to the following conclusions.

First, location and movement data processed through geographic information systems may give rise to legal relationships concerning the protection of personal non-property rights where such information enables the direct or indirect identification of individuals.

Second, the scholarly perspectives of H. Li, J. Huang, M.-P. Kwan, M. Malekzadeh, and other researchers demonstrate that geospatial data protection should extend beyond technical security measures to encompass the purposes of data processing, re-identification risks, and potential interference with individuals' private lives.

Third, European Union legislation establishes important legal safeguards for protecting personal non-property rights in geographic information systems, particularly through the principles of lawfulness, purpose limitation, data minimization, and effective mechanisms for restoring violated rights.

Fourth, the United States' experience highlights the importance of defining clear legal limitations on

World Bulletin of Management and Law (WBML)
Available Online at: https://www.scholarexpress.net
Volume-63 October-2026
ISSN: 2749-3601

government access to geolocation data and preventing unjustified interference with the right to privacy.

Fifth, the legislation of the United Kingdom and China provides valuable comparative legal approaches to distinguishing the liability of data controllers and processors, ensuring enhanced protection of sensitive personal information, and improving mechanisms for compensation for damage.

Sixth, an effective civil-law framework for protecting personal non-property rights in geographic information systems should integrate preventive measures, remedies for restoring violated rights, and mechanisms for compensating damage.

Seventh, it is advisable to improve Uzbekistan's legislation by establishing specific safeguards for geolocation data processing, clarifying the obligations of data controllers, introducing mechanisms for assessing re-identification risks, and strengthening legal remedies for violations of personal non-property rights.

Overall, improving the civil-law framework for protecting citizens' personal non-property rights in geographic information systems will contribute to achieving an appropriate balance between the effective use of digital technologies and the protection of individuals' right to privacy.

REFERENCES

1. Li H., Huang J., Kwan M.-P. Challenges in Geoprivacy Protection: Methodological Issues, Cultural and Regulatory Contexts, and Public Attitudes // Transactions in GIS. - 2025. - Vol. 29. - Article e70075. https://doi.org/10.1111/tgis.70075
2. Malekzadeh M., Kestens Y., Blanford J.I., Perchoux C., Mostafavi M.A., McKenzie G., Kim E.-K. Ethical Guidelines for Geoprivacy: A Framework for Researchers and Ethics Committees // International Journal of Health Geographics. - 2026. - Vol. 25. - Article 23. https://doi.org/10.1186/s12942-026-00460-y
3. Civil Code of the Republic of Uzbekistan (Part One). - 21 December 1995. - Articles 99–100. https://lex.uz/docs/111189
4. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). - Articles 4, 5, 6, 17, 25, 82. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
5. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 (Law Enforcement Directive). - Article 56. https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng
6. Stender S. Circumventing the Fourth Amendment: The Unconstitutional Nature of Geofence Warrants // Utah Law Review. - 2024. - No. 3. - P. 733–760. https://dc.law.utah.edu/ulr/vol2024/iss3/5/
7. Data Protection Act 2018 (United Kingdom). - Section 169. https://www.legislation.gov.uk/ukpga/2018/12/section/169
8. Personal Information Protection Law of the People's Republic of China. - 2021. - Articles 28, 69. https://en.spp.gov.cn/2021-12/29/c_948419_3.htm
9. Civil Code of the Republic of Uzbekistan (Part Two). - 29 August 1996. - Articles 985, 1021–1022. https://lex.uz/docs/180552
10. Law of the Republic of Uzbekistan No. ZRU-547 of 2 July 2019 "On Personal Data." https://lex.uz/docs/4396428
11. Court of Justice of the European Union. Judgment of 20 June 2024, AT and BT v PS GbR and Others, Case C-590/22, ECLI:EU:C:2024:536. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0590
12. Resolution No. 21 of the Plenum of the Supreme Court of the Republic of Uzbekistan dated 24 November 2025, "On Judicial Practice in the Application of Legislation on the Protection of Personal Non-Property Rights and Other Intangible Benefits." https://lex.uz/uz/acts/-7901164