Omega Journal of Legal Studies and Policy
ISSN: 3072-4686
Volume 01, Issue 03, June, 2026
Website: https://omegajournals.org

LEGAL CONCEPTS OF CROSS-BORDER DATA PROTECTION IN UZBEKISTAN

Shakhnoza Ibragimova
Judge of Yakkasaroy Interdistrict Civil Court of Tashkent
Tashkent, Uzbekistan
E-mail: sh.ibragimova@gmail.com

Abstract
This article examines the principal theoretical concepts underpinning the legal regulation of cross-border data flows, grouping them into three currents: the statist approach rooted in territorial sovereignty, the liberal-rights approach centred on fundamental rights, and technical normativism. Through comparative analysis of data protection legislation across the CIS states, the study identifies two competing regulatory models — the primacy of state control and liberal-rights integration — and situates Uzbekistan within this framework. Particular attention is given to the jurisprudence of the Court of Justice of the European Union on the right to erasure and adequacy, which reveals an unresolved tension between territoriality and universality. The article concludes that the dual character of personal data, simultaneously a constitutionally protected personal good and an object of economic circulation, constitutes the central theoretical problem of cross-border data law.

Keywords: Cross-border data transfer; data localisation; digital sovereignty; personal data protection; GDPR; right to erasure; adequate level of protection; CIS legislation; extraterritoriality.

Introduction

The global expansion of digital relations has generated a fundamentally new strategic problem of legal regulation for states. Norms developed within the framework of national jurisdiction are increasingly unable to regulate the growing flow of cross-border data effectively. Contemporary legal scholarship has proposed a number of theoretical concepts to address this problem, and these cluster around three ideological and methodological currents. The first is the

Omega Journal of Legal Studies and Policy
ISSN: 3072-4686
Volume 01, Issue 03, June, 2026
Website: https://omegajournals.org

'statist' approach, which rests upon the notions of state sovereignty and territorial control; the second is the 'liberal-rights' approach, which identifies the fundamental rights of the individual as the governing criterion; and the third is the 'technical normativism' approach, which treats the information-technology infrastructure as the basis of legal regulation.

The principal aim of this section is to examine, by legal-analytical methods, the theory of state sovereignty and the legal equilibrium of data localisation, data protection within the framework of the human rights concept, the theory of information as a public good, the principle of *lex informatica* in digital relations, and the concept of 'data nationalism'. The national legislation currently in force governing data-related matters, together with the legislation of the CIS states, is analysed under each of these concepts.

1. State Sovereignty and Data Localisation

The theory of state sovereignty, as the historical foundation of international law, was elaborated by Jean Bodin in the sixteenth century and Thomas Hobbes in the seventeenth, and was introduced into international practice through the Westphalian system.[1] In its traditional understanding, state sovereignty is characterised by three criteria: absolute authority within its own territory, the principle of non-interference in the internal affairs of other states, and equality of rights in external relations. Digital transformation, owing to the deterritorialised nature of 'cyberspace', has required all of these criteria to be understood in a substantially new manner.

In response to this situation, the concept of 'digital sovereignty' emerged. Jack Goldsmith and Tim Wu demonstrated that sovereignty in the digital environment is exercised through mechanisms of state control.[2] The notion of 'data localisation' is grounded as a legal instrument for consolidating digital sovereignty. By requiring that data pertaining to its citizens be stored on physical infrastructure located within its jurisdiction, the state secures control over that data. Data localisation regimes have been implemented in various legal forms across the world's major states.

In the Russian Federation, for example, article 242.1 of the Federal Law on Information, Information Technologies and the Protection of Information[3] made it mandatory to store the personal data of Russian citizens exclusively on servers

Omega Journal of Legal Studies and Policy
ISSN: 3072-4686
Volume 01, Issue 03, June, 2026
Website: https://omegajournals.org

situated in Russian territory. Breach of this norm results in the blocking of the data operator through its entry in the relevant register. Other CIS states have likewise developed distinctive legislative regimes on data localisation. In the Republic of Kazakhstan, the Law on Personal Data and its Protection[4] established localisation requirements analogous to the Russian model and provides for legally binding reporting by data operators within Kazakh territory in the course of personal data processing. In the Republic of Belarus, the Law on Personal Data,[5] adopted in 2021, established a data localisation regime consistent with Russian and Kazakh standards. At the same time, that law is among the acts that most fully entrench the protective rights of data subjects within CIS standards.

The Republic of Azerbaijan, the Republic of Armenia and Georgia display comparatively divergent approaches to data protection within the CIS region. In the Republic of Azerbaijan, the Law on Personal Data,[6] adopted in 2010, brought cross-border data transfer under state control. Localisation requirements are, however, framed less stringently than under the Russian or Kazakh models. In the Republic of Armenia, the Law on Personal Data[7] embodies a consistent programme of reform directed towards convergence with European Union standards; by introducing an 'adequate level of protection' criterion for cross-border transfers, Armenia exhibits the approach closest to the GDPR among the CIS states. Georgia has constructed a legal system built upon Council of Europe Convention 108 and GDPR principles pursuant to its Law on Personal Data Protection.[8] Arising from its 2014 Association Agreement with the European Union, Georgia has assumed an obligation to align with EU standards in the field of data protection.

Comparative analysis of the experience of the CIS states shows that these states have sought to employ one of two principal models in regulating cross-border data: the 'primacy of state control' model and the 'liberal-rights integration' model. Russia, Belarus and Kazakhstan, as representatives of the first model, have pursued a course of strengthening localisation requirements, whereas Armenia and Georgia, as representatives of the second, are pursuing a policy of convergence with European legal standards. Azerbaijan may be characterised as a 'transitional' model seeking to maintain a balance between the two directions.

Liability and sanction mechanisms also differ across the CIS states. In the Russian Federation, fines for breach of the data localisation regime were sharply increased

Omega Journal of Legal Studies and Policy
ISSN: 3072-4686
Volume 01, Issue 03, June, 2026
Website: https://omegajournals.org

from 2022, being set at 18 million roubles for each systemic violation. In Belarus, the institution of administrative liability was expanded under the 2021 law and the inspection powers exercisable over data operators were strengthened. In Kazakhstan, systemic supervision is carried out by the Republic's data protection committee. In Armenia and Georgia, independent data protection authorities operate on the basis of powers analogous to the European model, and reforms continue on the basis of Council of Europe recommendations. In the Republic of Uzbekistan, article 22 of the Law on Personal Data[9] has established the normative basis for cross-border data transfer; the absence, however, of criteria determining an 'adequate level of protection' and of a list of states complicates the practical application of that norm. Establishing an independent supervisory authority to secure accountability in the field of data protection, and defining its powers precisely, ought to be the next significant legal step for Uzbekistan.

With a view to resolving these tensions, the concept of 'balanced sovereignty' has been developed in the literature. The European Union's GDPR[10] offers the most refined legal model of such a balance: it does not mandate the retention of data within the country, but makes transfer to third countries conditional upon the criterion of an 'adequate level of protection'. Justifying data localisation as an absolute legal instrument, by contrast, gives rise to conflict with obligations under the World Trade Organization's General Agreement on Trade in Services.[11] Localisation restrictions may be assessed as an 'unnecessary barrier to trade', and studies indicate that data localisation regimes may reduce gross domestic product by between 0.1 and 1.7 per cent.[12]

2. Data Protection within the Human Rights Framework

Grounding data protection within the human rights tradition constitutes the most coherent conceptual line from a legal-philosophical standpoint. Article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights[13] entrench the right to respect for private life. Personal data is construed as an inseparable component of that right, and its processing and cross-border transfer are regarded as a distinct form of interference with private life.

The researchers Paul De Hert and Serge Gutwirth classify data protection as a fundamental right independent of privacy. On their account, the data protection

Omega Journal of Legal Studies and Policy
ISSN: 3072-4686
Volume 01, Issue 03, June, 2026
Website: https://omegajournals.org

system rests upon such distinctive principles as proportionality, purpose limitation, data minimisation and accountability.[14] Articles 7 and 8 of the Charter of Fundamental Rights of the European Union entrench these rights separately, as the right to private life and the right to the protection of personal data respectively.[15]

Across the CIS states, the human rights orientation has been absorbed into data protection legislation to varying degrees. In the Republic of Armenia, article 5 of the Law on Personal Data expressly establishes the data subject's right to private life as an independent constitutional guarantee, an approach that distinguishes Armenia as the state that has most fully implemented the human rights orientation in its legislation among CIS countries. In Georgia, article 3 of the Law on Personal Data Protection entrenches data protection as a constitutional right and has established the office of an independent Personal Data Protection Inspector. In Kazakh and Belarusian legislation, by contrast, the right to protection of personal data is regulated largely from the standpoint of administrative regulation, with the human rights foundation relegated to secondary importance.

In practical terms, through the judgments delivered by the Court of Justice of the European Union in *Schrems I* (2015) and *Schrems II* (2020),[16] the United States regulatory arrangements known as the 'Safe Harbour' and 'Privacy Shield' frameworks were held invalid on the ground that they failed to secure an adequate level of protection for the rights of EU citizens. Those judgments confirmed that human rights norms possess legal force beyond the boundaries of their own jurisdiction, and that protective requirements entrenched in one state may serve as a legal basis for prohibiting the transfer of data to another.

At the same time, from a theoretical standpoint, the 'right to erasure' model constitutes the practical expression of the human rights orientation. The Court of Justice of the European Union first formalised this right in judicial practice through its 2014 judgment in *Google Spain*. The substance of that case lay in the demand by a Spanish citizen, Mario Costeja González, that outdated information concerning him be erased from the Google search engine. The Court held that search engine operators are obliged to remove information from search results irrespective of its continued presence on the source website. The legal significance of this ruling lies in its confirmation of the individual's right to bring

Omega Journal of Legal Studies and Policy
ISSN: 3072-4686
Volume 01, Issue 03, June, 2026
Website: https://omegajournals.org

an independent claim against a disseminator of information; the 'right to erasure' subsequently received normative entrenchment in article 17 of the GDPR.[17]

The unbounded scope of application of this right, however, gave rise to a new legal problem. The French data protection authority (CNIL) required Google to give effect to erasure requests not only across European domain segments but across all domain segments worldwide, including google.com and google.co.jp. The Court of Justice of the European Union rejected that requirement, explaining that the 'right to erasure' operates within the territory of the European Union and applies for the benefit of the citizens of its Member States. It further concluded that the criterion is not mandatory on a global scale.[18] The particular significance of that judgment is manifest in two respects:

– first, it confirmed that the principle of territoriality in digital law may be applied even in relation to global platforms;

– secondly, by determining that one state's protective requirements ought not to possess binding force over another state's data flows, it left open the legal tension between national protective standards and global digital services.

Even so, this line of case law has not fully resolved the legal balance between the principles of territoriality and universality. In particular, the questions of the territory in which one state's erasure order is to be enforced, and whether that order acquires binding force in relation to other states, are not clearly regulated in international law. As a result, a data subject may demand only that information concerning them be erased in certain countries; on a global scale, such protection remains unsecured. This demonstrates that no generally recognised international legal mechanism has been developed to resolve the tension in cross-border data law between the individual's right to protection and the state's territorial jurisdiction.

Article 27 of the Constitution of the Republic of Uzbekistan guarantees the right to inviolability of private life. Article 31 of the Constitution, moreover, directly entrenches the right to protection of personal data as an independent constitutional guarantee. Under that article, everyone has the right to demand the protection of data concerning them, the rectification of inaccurate data and the destruction of data collected unlawfully.

In this sense, the Constitution of Uzbekistan has elevated the existing protection of personal data to the level of an independent fundamental right, in a manner

Omega Journal of Legal Studies and Policy
ISSN: 3072-4686
Volume 01, Issue 03, June, 2026
Website: https://omegajournals.org

close in substance to article 8 of the European Union's General Data Protection Regulation, and this lays the foundation for the development of cross-border data law in the country. Giving full effect to this constitutional basis through the norms of the Law of the Republic of Uzbekistan on Personal Data — in particular, through norms clarifying the procedure for cross-border transfer — remains a pressing task of legislative reform.

3. Information as a Public Good

At the same time, the significance of personal data not merely as an object of protection but also as an independent value in economic circulation calls for examination of the 'information as a public good' theory. That theory took shape as a result of transposing a category of economic science into the field of law, and characterises a public good by reference to two criteria: non-rivalry and non-excludability. For information, the criterion of non-rivalry is satisfied absolutely, since one subject's use of data does not diminish the ability of others to use it. Excludability, by contrast, is created artificially through copyright and data ownership regimes. Personal data, however, cannot fully satisfy both criteria, since it is simultaneously a personal good under constitutional protection and an object of circulation in the digital economy. It is precisely this dualism that constitutes the principal theoretical problem in determining the legal balance, in cross-border data law, between protecting the individual and securing the free flow of data.

Conclusion

The foregoing analysis permits several conclusions.

First, none of the three theoretical currents identified at the outset is capable, on its own, of furnishing an adequate framework for the regulation of cross-border data flows. The statist approach secures control but at the cost of economic efficiency and international trade obligations; the liberal-rights approach establishes coherent normative foundations but encounters the limits of territorial enforcement; and technical normativism addresses infrastructure without resolving questions of legitimacy. The regulatory task therefore lies not in choosing between these currents but in constructing a legal equilibrium among them.

Omega Journal of Legal Studies and Policy
ISSN: 3072-4686
Volume 01, Issue 03, June, 2026
Website: https://omegajournals.org

Secondly, comparative examination of the CIS states demonstrates that regional practice has bifurcated. The primacy-of-state-control model pursued by Russia, Belarus and Kazakhstan has produced increasingly stringent localisation requirements together with expanded sanction mechanisms, whereas the liberal-rights integration model followed by Armenia and Georgia has generated convergence with European standards, independent supervisory authorities and adequacy-based transfer regimes. Azerbaijan occupies an intermediate position. This divergence indicates that the CIS does not constitute a unified regulatory space in the field of data protection, and that any future harmonisation will require reconciling two structurally different regulatory philosophies.

Thirdly, the jurisprudence of the Court of Justice of the European Union has confirmed the extraterritorial reach of protective standards while simultaneously declining to universalise them. *Schrems I* and *Schrems II* established that domestic protective requirements may lawfully restrict outward data transfers; *Google Spain* and the subsequent *CNIL* judgment established that they may not be projected globally. The consequence is a structural asymmetry: a state may prohibit the export of data yet cannot secure the protection of that data once exported. International law has not yet produced a mechanism capable of resolving this asymmetry.

Fourthly, the constitutional foundation for data protection in Uzbekistan is soundly established. Article 31 of the Constitution elevates the protection of personal data to an independent fundamental right, in substance approaching the standard articulated in article 8 of the Charter of Fundamental Rights of the European Union. The legislative implementation of that guarantee, however, remains incomplete. Article 22 of the Law on Personal Data provides a normative basis for cross-border transfer but lacks the two elements necessary to render it operative: criteria defining an adequate level of protection, and a corresponding list of states satisfying those criteria. It is accordingly proposed that (a) adequacy criteria be adopted at the level of a governmental decision, drawing upon the methodology of article 45 of the GDPR; (b) a list of states affording an adequate level of protection be approved and periodically reviewed; and (c) an independent supervisory authority for data protection be established, with clearly delimited powers of inspection, enforcement and adequacy assessment.

Omega Journal of Legal Studies and Policy
ISSN: 3072-4686
Volume 01, Issue 03, June, 2026
Website: https://omegajournals.org

Finally, the theory of information as a public good exposes the deepest conceptual difficulty in this field. Personal data is neither purely a protected personal good nor purely an object of economic circulation, but both at once. So long as legal doctrine continues to treat these two characterisations as alternatives rather than as concurrent attributes of a single object, cross-border data law will remain internally inconsistent. The elaboration of a regulatory model capable of accommodating this dualism — protecting the individual without obstructing the flow of data — constitutes the principal task for further research.

References

1. Jean Bodin, Les Six Livres de la République (Jacques du Puys 1576); Thomas Hobbes, Leviathan (Andrew Crooke 1651).
2. Jack Goldsmith and Tim Wu, Who Controls the Internet? Illusions of a Borderless World (OUP 2006).
3. Federal Law No 149-FZ of 27 July 2006 'On Information, Information Technologies and the Protection of Information' (Russian Federation), art 242.1. [Note: art 242.1 is in fact located in Federal Law No 242-FZ (2014) amending art 18(5) of Law No 152-FZ 'On Personal Data' — please verify the intended provision.]
4. Law of the Republic of Kazakhstan No 94-V of 21 May 2013 'On Personal Data and its Protection'.
5. Law of the Republic of Belarus No 99-Z of 7 May 2021 'On the Protection of Personal Data'.
6. Law of the Republic of Azerbaijan No 998-IIIQ of 11 May 2010 'On Personal Data'.
7. Law of the Republic of Armenia HO-49-N of 18 May 2015 'On the Protection of Personal Data'.
8. Law of Georgia No 5669-Iს of 14 June 2023 'On Personal Data Protection'.
9. Law of the Republic of Uzbekistan No ZRU-547 of 2 July 2019 'On Personal Data', art 22.
10. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1.

Omega Journal of Legal Studies and Policy
ISSN: 3072-4686
Volume 01, Issue 03, June, 2026
Website: https://omegajournals.org

11. General Agreement on Trade in Services (adopted 15 April 1994, entered into force 1 January 1995) 1869 UNTS 183.
12. [Study author], '[Title]' ([Publisher/Journal] [year]) [pinpoint].
13. Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III)) art 12; International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171, art 17.
14. Paul De Hert and Serge Gutwirth, 'Privacy, Data Protection and Law Enforcement: Opacity of the Individual and Transparency of Power' in Erik Claes, Antony Duff and Serge Gutwirth (eds), Privacy and the Criminal Law (Intersentia 2006) 61.
15. Charter of Fundamental Rights of the European Union [2012] OJ C326/391, arts 7–8.
16. Case C-362/14 Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650; Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems [2020] ECLI:EU:C:2020:559.
17. Case C-131/12 Google Spain SL v Agencia Española de Protección de Datos [2014] ECLI:EU:C:2014:317; GDPR, art 17.
18. Case C-507/17 Google LLC v Commission nationale de l'informatique et des libertés (CNIL) [2019] ECLI:EU:C:2019:772.