# LEGAL GUARANTEES FOR THE PROTECTION OF PETITIONERS' PERSONAL DATA AND FOR PROTECTION AGAINST CYBER-HARASSMENT UNDER CONDITIONS OF DIGITAL ALGORITHMS

**Akmaljon Isabayev**
*Chief Consultant, Department for the Analysis of Constitutional Legislation, Constitutional Court of the Republic of Uzbekistan, PhD*

**Abstract:** This article analyses the constitutional guarantees needed to protect petitioners' personal data and to shield them from cyber-harassment where public authorities process electronic petitions through algorithmic systems. Automated sorting and AI-based processing of petitions generate risks — algorithmic discrimination, data breaches and doxxing — that national legislation addresses only in fragments. Using comparative-legal, normative-dogmatic and systemic-functional methods, the article argues that data security and procedural safeguards against automated decisions are constituent elements of the right to petition rather than external conditions of it, and proposes a four-stage protective model: preventive, procedural, cyber-protective and remedial. Concrete legislative proposals follow.

**Keywords:** digital state, algorithmic governance, right to petition, personal data, cybersecurity, digital rights, artificial intelligence.

## Introduction

The digitalisation of public administration—particularly in the handling of citizens' petitions—has entered a qualitatively new phase in recent years. The steady growth in the volume of electronic petitions is pushing state bodies toward automated systems, including artificial-intelligence algorithms, for sorting and distributing them. Yet this process has a second, still under-examined side: as an algorithm processes a petitioner's data, its intrusion into that person's private life creates risks that did not previously exist. These include automatically labelling a petitioner as "high-risk" on the basis of their data (algorithmic discrimination), unlawful exposure of personal data from databases, and subjecting a person to doxxing, cyber-stalking, or other forms of digital pressure precisely because they filed a petition.

The problem is compounded by the fact that the relevant national laws — on petitions, on personal data and on cybersecurity — each operate within their own subject matter, while no comprehensive regime governs the risks arising specifically at their intersection. As Ryan Calo has shown, artificial-intelligence technologies pose a fundamentally new challenge for administrative law: the

traditional categories of authority, liability and oversight do not map cleanly onto automated decision-making. The research problem is accordingly framed as follows: how can the security of petitioners' personal data and their protection from cyber-harassment be justified as an integral, autonomous guarantee of the right to petition, and through which model can this be secured?

The study proceeds from human dignity as the common constitutional foundation of every institution examined below, and follows the chain: human dignity — the right to petition — personal-data security — digital security — artificial intelligence — algorithmic fairness.

Chapter I. The Legal Nature of the Right to Petition in the Digital Environment

**1.1. Constitutional content**

The right to petition, enshrined in Article 40 of the Constitution of the Republic of Uzbekistan, has a dual significance within the human-rights system—both procedural and substantive: it covers not only the citizen's ability to communicate with the state, but also the requirement that any personal data used in that communication be processed lawfully and securely. As O. Khusanov notes, the modern understanding of constitutional rights encompasses not merely the state's negative duty of non-interference but also its positive duty actively to secure citizens' rights. In the context of data security this positive duty is especially significant, since a state body accepting a petition must take active measures to protect the petitioner's data, failing which the right to petition itself becomes merely formal.

The principle of proportionality carries particular methodological weight: the volume of data a state body collects about a petitioner, and the manner of its processing, must be proportionate to the purpose of examining the petition. This follows from the constitutional recognition of human dignity as the supreme value: if an algorithm treats a petitioner merely as a "data set" without regard to their individual circumstances, the citizen ceases to be a subject of the administrative process and becomes its object. As A.B. Gafurov observes, the digitalisation of state institutions is not an end in itself but a means of building governance that secures human rights.

1.2. Legal features of electronic petitions

An electronic petition differs fundamentally from a traditional written one: it comes bundled with electronic identification (e.g., through the ONE ID system), automatic registration, and a "digital footprint"—IP address, device identifier, timestamp, and other metadata. As A.D. Gofurov shows, digitalisation reduces the discretionary latitude of an individual official within an agency and standardises the process, but this very standardisation sharply increases the volume of data collected, correspondingly heightening the need to

protect it.

1.3. The concept of algorithmic governance

In the international literature, “algorithmic governance” denotes the making of state decisions through partially or fully automated systems. As E. Talapina has shown, such systems generate probabilistic assessments of individuals, which may violate the right to individualised, fair consideration.^7 In the petitions context, an algorithm that classifies a petitioner as a “frequent complainant” on the basis of their petition history may affect the handling of future petitions and amount to concealed discrimination. Lessig's formula that “code is law” applies directly: where algorithmic code escapes legal oversight, it becomes in practice a stronger regulatory force than statute.

Chapter II. Legal Foundations for Protecting Petitioners’ Personal Data

2.1. The legal regime of personal data

The Law “On Personal Data” (No. ZRU-547, 2 July 2019) establishes the general procedure for processing personal data, but contains no specific rule on the automated processing or sorting of petitions. In foreign practice this gap is filled by the EU General Data Protection Regulation: its Article 22 establishes an individual’s right not to be subject to a decision based solely on automated processing that produces legal effects concerning them. The Council of Europe’s modernised Convention 108+ extends a similar right beyond the regional level to a broader international scale, while the OECD Privacy Guidelines remain significant as the first instrument to articulate the principles of data minimisation and purpose limitation.

2.2. Categories of data processed during petition handling

An electronic petition typically involves processing of the petitioner's name, contact details, IP address and, occasionally, geolocation and biometric data. In S. and Marper v. United Kingdom the European Court of Human Rights held that indefinite retention of biometric data may violate the right to privacy, and in Big Brother Watch and Others v. United Kingdom it emphasised that bulk interception regimes must be subject to rigorous oversight and robust safeguards. Both conclusions apply to biometric and monitoring data within petition systems.

A petition system also retains a citizen's entire petition history, which over time forms a detailed profile of their social and legal activity; this profile becomes the basis for algorithmic analysis and must therefore be assessed as personal, not merely administrative, information. As V. Mayer-Schönberger and K. Cukier show, aggregate analysis of individually harmless facts may reveal more personal information than any single data point.^16

2.3. Principles of data processing

The principles enshrined in the GDPR and in national law —

minimisation, purpose limitation, proportionality, transparency and accountability — require a petition system to collect only the data necessary to examine the petition, to use it solely for that purpose, to retain it for a proportionate period, to keep the petitioner informed, and to hold the responsible agency accountable.

The theoretical foundation of these principles lies in J. Cohen's concept of "informational privacy": privacy, in her view, is not simply concealment of information but the ability to control how one's own social "profile" is formed. N. Richards, through the concept of "intellectual privacy," shows that a person who senses they are being observed loses the capacity to think and act freely—a conclusion of particular relevance to petitioners: if a citizen knows their petitions are continuously monitored and profiled by an algorithm, this may chill their future willingness to petition at all.

Chapter III. Legal Risks Arising from Digital Algorithms

3.1. Algorithmic discrimination

Bias, profiling, ranking and filtering constitute the four principal mechanisms of algorithmic discrimination. Talapina has demonstrated that algorithmic transparency is central to AI ethics in public administration, since the "black box" problem threatens the institution of legal accountability. K. Yeung observes that the legitimacy of such systems is built not upon open, contestable rules but upon a continuously shifting data stream, which challenges traditional mechanisms of legal oversight, and F. Pasquale shows that their internal logic may remain opaque even to oversight bodies, undermining democratic accountability.

As a legal remedy, S. Wachter, B. Mittelstadt, and C. Russell proposed the method of "counterfactual explanations": without disclosing an algorithm's full internal logic, it is possible to provide the explanation "had X been different, the outcome would have been different too," which in practice satisfies the explainability requirement of GDPR Article. This problem is especially acute for petitioners: if a petitioner cannot learn why their application was marked "low priority" or had its deadline extended, they cannot effectively defend their rights.

3.2. Data breaches

Data breaches, cloud-infrastructure risks and unauthorised third-party access are hazards associated with the centralised storage of petition databases. As S. Zuboff shows, the accumulation of personal data may become a means of exercising indirect power over the data subject — a conclusion equally applicable to state databases, whose uncontrolled expansion risks turning them into an informal instrument of control. A. Khalmuratov has shown, using Uzbekistan as an example, that phishing and cyber-extortion remain

insufficiently addressed in legislation, weakening the principle of the inevitability of punishment.

3.3. The concept of cyber-harassment

The scholarly typology of cyber-harassment includes doxxing (the non-consensual public disclosure of private information), cyber-stalking, online intimidation, revenge publication and identity theft. D. Citron shows that cyber-harassment is a serious offence with direct consequences for a victim's employment, family and physical safety, and that treating it merely as an “online dispute” is a trivialising approach. The typology matters legally because it distinguishes the objective element of each form, allowing correspondingly distinct responses — a right to erasure for doxxing, monitoring and blocking for cyber-stalking.

3.4. Digital forms of retaliation against petitioners

The most dangerous scenario in practice is digital pressure directed at a person precisely because they filed a petition: unlawful disclosure of the petitioner's data, algorithmic labelling as a “problem individual,” or misuse of state registries against them. Such conduct produces a chilling effect on the right to petition — fearing that their data is unprotected, a citizen may abandon even a well-founded complaint.

Chapter IV. International Standards and Foreign Experience

4.1. International instruments

Article 12 of the Universal Declaration of Human Rights enshrines the right to privacy in general terms, a right that applies fully to the digital environment; Article 17 of the International Covenant on Civil and Political Rights states the same prohibition on arbitrary interference in binding form. UN General Assembly Resolutions 68/167 and 69/166 affirm that rights enjoyed offline must be equally protected online, with particular attention to unlawful mass surveillance, and the Council of Europe's Convention 108 established the first binding standards for automated processing and cross-border transfers.

4.2. European Union experience

The GDPR sets the general standard for personal-data protection, while the EU Artificial Intelligence Act (Regulation (EU) 2024/1689) establishes requirements of human oversight and transparency for high-risk AI systems used in public services.^27 The NIS2 Directive (EU) 2022/2555 sets minimum cybersecurity obligations for public bodies, including incident-notification deadlines.^28 Together, these three instruments form a single legal chain linking personal-data security, algorithmic transparency, and cyber-protection within petition systems.

4.3. Foreign national experience

In Germany, administrative digital services are subject to the data-protection-by-design principle of Article 25 GDPR.^29 Estonia's Information System Authority operates a “Data Tracker,” which logs every query made to a state database and allows citizens to see, via the eesti.ee portal, who accessed their data, when and for what purpose.

In the Republic of Korea, the Personal Information Protection Commission (PIPC), which became an independent central authority after the 2020 reform, has the power to inspect and audit the automated systems used by state agencies. Singapore’s experience requires a qualification: under the “Smart Nation” programme, the “AI Verify” testing tool exists, but this is not a mandatory state audit; rather, it is a voluntary instrument enabling organisations to assess their own algorithms against internationally recognised criteria.^32 These experiences show that, regardless of the level of technical development, independent oversight and formalised procedure play a vital role in every system—though whether such a mechanism is mandatory (Germany, Korea) or voluntary (Singapore) materially affects its practical effectiveness.

Chapter V. Legal Guarantees and Existing Gaps in Uzbek Legislation

5.1. Analysis of current legislation

Article 31 of the Constitution guarantees the inviolability of private life and the protection of personal data, while Article 40 guarantees the right to petition. The Law “On Petitions of Individuals and Legal Entities” governs petition-handling procedure; the Law “On Personal Data”^33 governs its general processing regime; and the Law “On Cybersecurity” (No. ZRU-764, 15 April 2022) establishes the state system for the cyber-protection of information systems.^34 These three laws, however, operate independently of one another—there is no dedicated regime addressing their intersection within the petition process, an omission that impedes the formation of a single, integrated system for cybersecurity and data protection within petition handling.

5.2. Legal gaps

The analysis identifies five gaps. First, no special procedure governs the use of artificial intelligence in processing petitions in state bodies. Second, the explainability of algorithm-based decisions is not legally guaranteed. Third, there is no simplified, dedicated mechanism for appealing automated decisions. Fourth, “cyber-harassment” has no precise legal definition in national law, appearing instead in fragmented form across various statutes. Fifth, no dedicated digital protection measures, such as an anonymised complaint channel, are envisaged for petitioners. As a result, the principle of inevitability of liability for information-security offences remains incompletely secured.

5.3. Practical problems

Beyond these normative gaps, practice reveals uncontrolled expansion of

inter-agency data-sharing, insufficient information-security competence among staff, and the absence of a clear liability system for data leaks; as Khalmuratov notes, the shortage of qualified IT specialists in law-enforcement bodies deepens these problems.^35 Addressing them requires a unified legal mechanism governing inter-agency data exchange and a clearly defined liability for each state body in cases of violation of personal-data inviolability.

Chapter VI. A Legal Model for Protecting Petitioners' Personal Data

Building on the foregoing analysis, the author proposes the concept of "Digital Procedural Security of Petitioners" and a four-stage legal model combining preventive, procedural, cyber-technical and remedial safeguards in sequence, each stage compensating for the potential failure of the one before it.

- **I. Preventive safeguards:** data encryption, data minimisation, privacy by design, and privacy impact assessment—measures aimed at eliminating risk before a system is deployed.
- **II. Procedural safeguards: notification that an algorithm is being applied (explainability); the right to human review of an automated decision (human oversight); the duty to give reasons (accountability); the right to contest and demand reconsideration (contestability); and independent electronic audit. These five elements are mutually dependent: without explainability, contestability is meaningless; without human oversight, accountability is merely formal.**
- **III. Cyber protection:** anonymisation and pseudonymisation of data, two-factor authentication, logging of all access and modifications, and continuous monitoring—measures that give practical effect to the proportionality and oversight requirements articulated in Big Brother Watch.^36
- **IV. Remedial safeguards:** the right to compensation where data has leaked or been unlawfully used; the right to erasure (a petition-system application of the "right to be forgotten"); digital rehabilitation (for example, revoking a "high-risk" status wrongly assigned by an algorithm); and the material and disciplinary liability of the responsible state body.

The model is systemic: if the preventive stage fails (for instance, excessive data is collected), the procedural stage should catch the failure; if that too fails, cyber protection should serve as a technical barrier; and, where harm

nonetheless occurs, the remedial mechanism must operate. No single safeguard is self-sufficient—each is a linked element of one continuous chain.

Chapter VII. Algorithmic Constitutionalism and the Doctrine of Digital Rights

The risks and safeguards examined above rest on a broader theoretical foundation — the doctrine of digital constitutionalism, which holds that state power remains bound by constitutional limits in the digital environment: an algorithm cannot become a new, law-free form of state authority. Following the framework proposed by L. Floridi and J. Cowls, AI systems must observe the principles of beneficence, non-maleficence, autonomy, justice and explicability — five principles that apply fully to petition-processing algorithms as constitutional-ethical limits. Two consequences follow. Where an algorithm exercises the state's executive function, it must comply with the principles of legality and proportionality; and the citizen's rights against an algorithmic decision — to an explanation, to object, and to demand human reconsideration — govern specifically the relationship between an individual and an automated system.

Algorithmic transparency and accountability are the instruments through which this doctrine becomes operational, but disclosure alone is insufficient: without an independent oversight institution, transparency remains declaratory. While administrative and parliamentary oversight monitor an algorithm's day-to-day operation, judicial — and specifically constitutional — review remains the final guarantee for examining the normative foundations affecting human rights. The compulsory nature of human oversight forms the practical core of digital constitutionalism: however far an agency's digitalisation extends, the final decision determining a petitioner's fate must remain within the sphere of human responsibility. An algorithm may only assist; it can never be the final arbiter.

**Conclusion**

This study shows that the effective exercise of the right to petition in the digital environment is inseparable from securing the petitioner’s personal data and protecting them from cyber-harassment; both should be regarded as integral, constituent guarantees of the right to petition itself. Although three sector-specific laws exist at the national level (on petitions, on personal data, and on cybersecurity), a regulatory gap persists precisely at their intersection—the algorithmic risks arising within the petition process itself.

The proposed four-stage model is, in essence, a practical expression of digital procedural justice: it secures the petitioner's right to fair treatment at every stage, from data collection to the execution of the final decision. The procedural-safeguards block applies the logic of algorithmic due process —

just as a traditional fair trial guarantees a right to be heard, an automated decision must guarantee the rights to a hearing, an explanation and contestation. The cyber-technical block, in turn, marks out a direction in which cybersecurity is recognised not as a purely technical function but as a constitutional-level means of protecting human rights.

As practical recommendations, the study proposes:

1. Introducing a dedicated provision in the Law "On Petitions of Individuals and Legal Entities" governing the automated processing of petitions, including a petitioner's right to human review;
2. Establishing a mandatory explainability requirement for algorithm-based decisions;
3. Introducing a single legal definition of "cyber-harassment" and creating an expedited administrative mechanism to combat it (for example, under the Ombudsman);
4. Establishing a clear system of material liability for state bodies in cases of data leaks from petition databases.

As a final methodological conclusion, the constitutional value of a digital state is determined not by the extent of its reliance on artificial intelligence, but by the degree to which such technologies protect human dignity, the inviolability of private life, and the right to petition. This is precisely the criterion that closes the logical chain set out in the Introduction—human dignity, the right to petition, personal data, digital security, artificial intelligence, algorithmic fairness—and it is this criterion that ultimately determines whether digital governance can be considered genuinely successful.

## REFERENCES

1. Ryan Calo, "Artificial Intelligence Policy: A Primer and Roadmap" (2017) 51:2 UC Davis Law Review 399–435.
2. Shavkat M. Mirziyoyev, "Speech at the Video Conference on Implementing the New Edition of the Constitution and Continuing Consistent Reforms", Khalq So'zi newspaper, 9 May 2023, No. 92.
3. Constitution of the Republic of Uzbekistan (new edition of 30 April 2023), Art. 40.
4. O.T. Khusanov, Constitutional Law: A Textbook (Tashkent: Adolat, 2022), 95–98.
5. A.B. Gafurov, "The Digitalisation of the Activities of the Constitutional Court of the Republic of Uzbekistan as an Important Condition for Ensuring Openness and Transparency" (2023) 4:100 Democratization and Human Rights Journal 88–97.

6. A.D. Gofurov, The Digital Economy and E-Government (Tashkent: TSLU, 2021), 312.
7. E.V. Talapina, "Data Processing Using Artificial Intelligence and the Risks of Discrimination" (2021) Legal Thought: History and Modernity (HSE electronic edition).
8. L. Lessig, Code: Version 2.0 (New York: Basic Books, 2006), 410.
9. Law of the Republic of Uzbekistan "On Personal Data", No. ZRU-547, 2 July 2019, online: <lex.uz/docs/4396419>.
10. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), Art. 22, 25.
11. Council of Europe, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+), CETS No. 223, 2018.
12. OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 1980 (revised 2013).
13. S. and Marper v United Kingdom [GC], Nos 30562/04 and 30566/04, [2008] ECHR.
14. Bărbulescu v Romania [GC], No 61496/08, [2017] ECHR.
15. Big Brother Watch and Others v United Kingdom [GC], Nos 58170/13, 62322/14 and 24960/15, [2021] ECHR.
16. V. Mayer-Schönberger & K. Cukier, Big Data: A Revolution That Will Transform How We Live, Work, and Think (New York: Eamon Dolan/Houghton Mifflin Harcourt, 2013), 242.
17. J.E. Cohen, Configuring the Networked Self: Law, Code, and the Play of Everyday Practice (New Haven: Yale University Press, 2012), 336.
18. N.M. Richards, Intellectual Privacy: Rethinking Civil Liberties in the Digital Age (Oxford: Oxford University Press, 2015), 256.
19. E.V. Talapina, "Transparency of Artificial Intelligence Algorithms" (2025) 18:3 Law. Journal of the Higher School of Economics 4–27.
20. K. Yeung, "Algorithmic Regulation: A Critical Interrogation" (2018) 12:4 Regulation & Governance 505–523.
21. F. Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information (Cambridge, MA: Harvard University Press, 2015), 320.
22. S. Wachter, B. Mittelstadt & C. Russell, "Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR" (2018) 31:2 Harvard Journal of Law & Technology 841–887.
23. S. Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (New York: PublicAffairs, 2019), 704.

24. A.O. Khalmuratov, "Legal Aspects of Enhancing Measures to Prevent and Counter Cybercrime in the Republic of Uzbekistan" (2026) 6:4 Eurasian Journal of Law, Finance and Applied Sciences 137–147.
25. D.K. Citron, Hate Crimes in Cyberspace (Cambridge, MA: Harvard University Press, 2014), 352.
26. Universal Declaration of Human Rights, UNGA, 10 December 1948, Art. 12.
27. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).
28. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (NIS2 Directive).
29. General Data Protection Regulation (GDPR), supra note 10, Art. 25.
30. Republic of Estonia Information System Authority (RIA), "Data Tracker", online: <ria.ee/en/state-information-system/people-centred-data-exchange/data-tracker>.
31. Personal Information Protection Commission (Republic of Korea), Personal Information Protection Act (PIPA) and the PIPC's 2020 institutional reform, online: <pipc.go.kr>.
32. Infocomm Media Development Authority and Personal Data Protection Commission (Singapore), Model Artificial Intelligence Governance Framework; AI Verify Testing Framework, online: <pdpc.gov.sg>.
33. Law "On Personal Data", supra note 9.
34. Law of the Republic of Uzbekistan "On Cybersecurity", No. ZRU-764, 15 April 2022, online: <lex.uz/docs/5960604>.
35. A.O. Khalmuratov, supra note 24, 140.
36. Big Brother Watch, supra note 15.
37. L. Floridi & J. Cowls, "A Unified Framework of Five Principles for AI in Society" (2019) 1:1 Harvard Data Science Review.