RKS Global

rks.global

Human vs Model: How Governments Use AI for Censorship and Surveillance

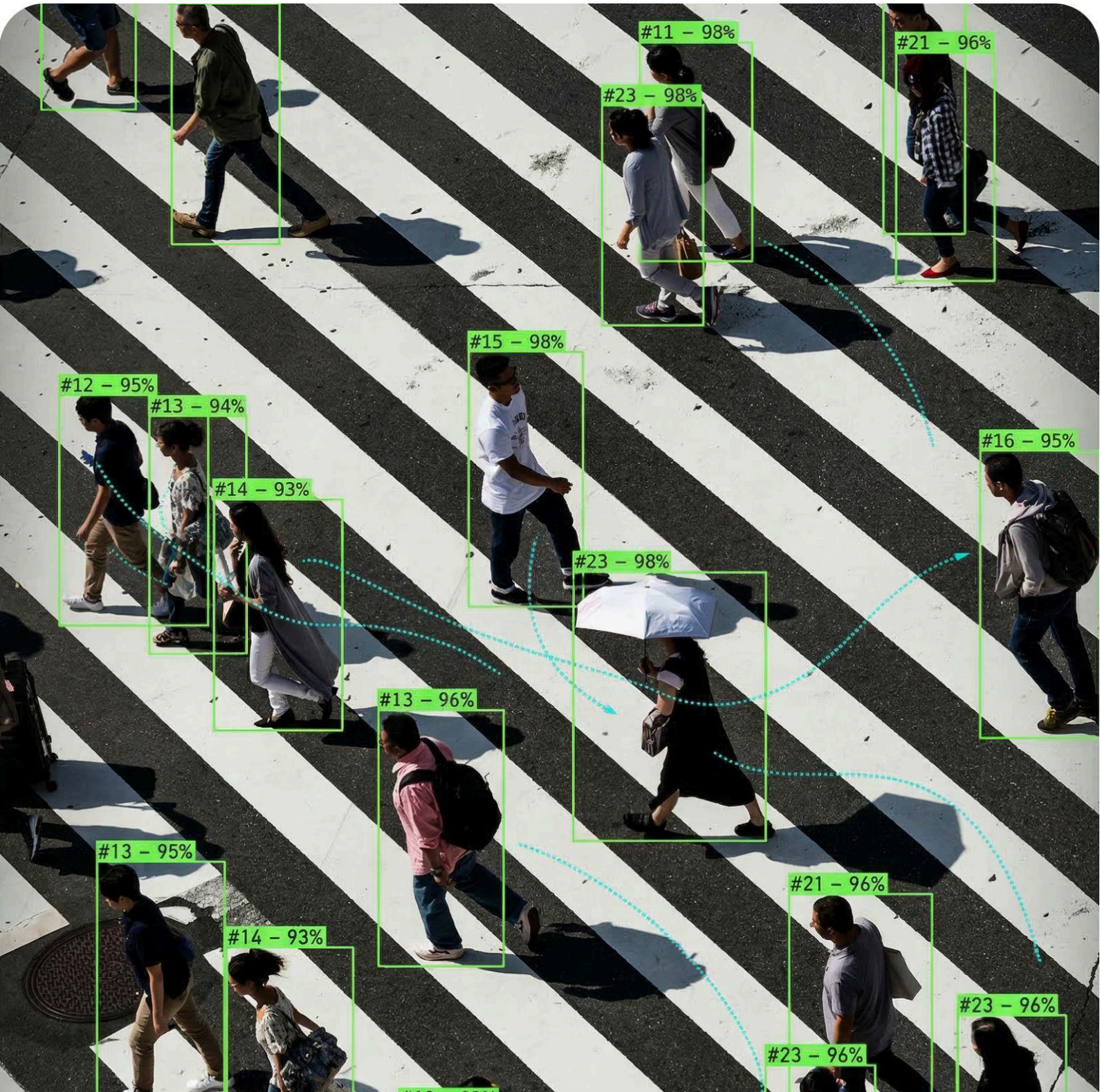

Table of contents

Introduction

The development of state-of-the-art AI systems and models is primarily driven by private companies and venture capital. However, government agencies also seek to participate in this race, developing and deploying new technologies for their own purposes. In many countries, AI systems are already being used in law enforcement, national defence, and security.

In many cases, the deployment of AI systems enables the government apparatus to accelerate its operations, improve quality, and reduce costs. Automation of routine processes, analysis of large datasets, and forecasting of social phenomena open new opportunities for public authorities to fulfil government functions. However, the positive effects of AI deployment are inextricably linked to significant risks to human rights and freedoms. Facial recognition systems, automated internet monitoring, and predictive analytics can be used not only to combat crime and maintain public order, but also to suppress political opposition, persecute dissenters, and establish total control over the population.

In this context, the situation in countries with authoritarian and hybrid political regimes is of particular concern. The absence of an independent judiciary, the weakness of civil society institutions, and the limited accountability of public authorities create conditions that tempt those in power to use the latest technologies to maintain control. Insufficient legal regulation of AI system development and deployment, and the absence of transparency mechanisms, are often masked by rhetoric about the need to stimulate innovation and support the technology sector. An additional factor is competition among leading technological powers seeking to extend their influence, including through the export of surveillance systems and digital infrastructure.

The main objective of the study is to examine the current state of regulatory frameworks governing the development and deployment of AI systems in selected Eurasian countries, analyse government investments in technological development, and systematise available information on the potential use of AI systems for online censorship, overt and covert surveillance.

The study is based on the analysis of open-source information, including normative legal acts, official strategic planning documents, reports from international and human rights organisations, media materials, and academic publications. In addition, interviews with experts who possess practical knowledge of AI system deployment practices in the respective jurisdictions were conducted.

Azerbaijan

Strategies and Legal Regulation

The principal strategic document is the AI Development Strategy for 2025–2028. It identifies five key areas, one of which is the development of AI legal regulation. Discussions regarding the content of future regulations are currently underway, and interested parties are submitting their proposals.

Further amendments to the Law “On Personal Data” are envisaged within the framework of digital technology regulation.

In January 2025, the Digital Development Concept was approved to accelerate economic development through digital technologies.

The Centre for Analysis and Coordination of the Fourth Industrial Revolution (C4IR), operating under the Ministry of Economy, coordinates and analyses initiatives and projects in the digital economy.

Funding and Strategic Projects

AI sector development is largely envisioned through funding for private companies and government agencies. The Innovation and Digital Development Agency (IDDA) coordinates the country’s digital transformation and startup ecosystem support.

ASAN AI Hub coordinates collaboration among the public sector, business, research centres, and the startup ecosystem in AI.

In December 2024, the European Investment Bank provided a loan of EUR 43 million for the construction of two Tier 3 data centres.

Use of AI Systems for Censorship

In Azerbaijan, public authorities may require the removal of unlawful content, or restrict access to an internet resource in accordance with Article 13.3 of the Law "On Information, Informatisation, and Protection of Information." If the provider fails to comply with the regulator's requirements, access may be restricted by court order. In urgent cases, access may be restricted by executive authorities' decisions, with subsequent judicial review. However, the blacklist of restricted resources is not publicly available. The activities of public authorities are sufficiently opaque to preclude assessment of whether AI systems are being used to identify unlawful content.

In accordance with Article 10 of the Law "On Operational-Investigative Activities," wiretapping of telephone conversations and extraction of information from communication channels do not require judicial authorisation or oversight by a superior authority, unless the installation of technical devices in a dwelling is contemplated. Freedom House in 2023 indicated that the technical capabilities of the System of Operational-Investigative Activities (SORM), including deep packet inspection (DPI) technology, were likely being used.

Azerbaijan systematically blocks independent media and restricts access to social networks, particularly during emergencies. For example, during conflicts and protests, access to certain internet resources and social networks was blocked.

Use of AI Systems for Overt and Covert Surveillance

Video surveillance installation in Azerbaijan is carried out as part of the "Safe City" project. According to 2023 data, approximately 15,000 cameras have been installed in the country. From a legal perspective, identification is carried out in accordance with the Law "On Biometric Information."
In November 2025, the President signed a decree establishing the

Centralised Information and Digital Analytics System MIRAS, which envisages integrating databases from various government agencies to create a unified digital portfolio for citizens. Human Rights Watch expressed concern that a centralised system consolidating sensitive personal data from various agencies in the absence of adequate independent oversight creates serious risks of arbitrary or disproportionate surveillance.

According to human rights organisations, government agencies have repeatedly used the Pegasus spyware. For example, according to Amnesty International, as of 2023, more than 1,000 Azerbaijani numbers had been selected for potential targeting by a Pegasus client.

Armenia

Strategies and Legal Regulation

The National AI Development Strategy in Armenia is currently being drafted and discussed. It is expected to focus primarily on the deployment of AI systems in specific areas of public life. The AI sector is subject to the country's general legislation. No specific legislative decisions have been announced yet.

Funding and Strategic Projects

In 2025, a $500 million public-private partnership with Firebird.ai was announced to create an AI-based supercomputer data centre with an estimated capacity of 100 megawatts.

In addition, at the beginning of 2025, a cooperation agreement was signed with French AI start-up Mistral AI in both the private and public sectors.

Furthermore, the government is implementing programmes to support entrepreneurs and start-ups in AI.

Use of AI Systems for Censorship

In accordance with the law, telecommunications operators must block websites that violate the law (primarily illegal casinos and gambling sites).

Certain telecommunications operators used selective blocking of social networks during the armed conflict in 2020.

Use of AI Systems for Overt and Covert Surveillance

In 2020–2022, a number of public figures were targeted using the Pegasus and Predator spyware; however, the specific clients have not been identified. Circumstantial evidence points to the use of Pegasus by Azerbaijani government agencies and Predator by Armenian ones.

In 2025, amendments to the Law “On Police” entered into force, granting police access to cameras in public places for biometric identification.

From 2017 to 2018, cameras and infrastructure were supplied by Chinese companies under the “Smart City” project; however, in recent years, there has been a shift toward cooperation with the United States and India.

Belarus

Strategies and Legal Regulation

Belarus lacks specific regulatory legislation governing AI; the industry is subject to general legislation. It is expected that conceptual documents and regulatory legal acts will begin to be developed in 2026.

In 2025, the State Program "Digital Belarus" for 2026–2030 was approved. Its key areas include developing government digital platforms and deploying data processing technologies, including AI.

In 2025, a working group of the UIIP NAS Belarus developed the CIS Model Law on Artificial Intelligence Technologies, which was adopted by the CIS Interparliamentary Assembly. The document itself is a compilation of selected provisions of the EU Artificial Intelligence Act (the AI Act) and the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. Since the document is effectively unenforceable in practice, the CIS states have not implemented it into national legislation.

In 2025, a standardisation committee "Digital Development and Communications" (TC DY 41) was also established. It is expected to develop technical standards in AI and to coordinate their alignment with Russian and international practices.

Funding and Strategic Projects

The key instrument for the development of the IT sector and AI technologies in the country remains the Hi-Tech Park, founded in 2005.

Several major Tier 3 data centres have been built in the country: the Republican Data Processing Centre (RDPC) operated by beCloud and the A1 data centre.[1]

In 2025, a project to build a large data centre powered by nuclear energy was discussed with Russian representatives.

Use of AI Systems for Censorship

Restriction of access to content and internet resources in Belarus is carried out pursuant to Article 51[1] of the Law "On Mass Media," which provides for extrajudicial blocking by decisions of the Ministry of Information (and other agencies) or by prosecutors' orders. The list of information prohibited from dissemination is contained in Article 38.

The second law on the basis of which internet censorship is carried out is the Law "On Countering Extremism." It permits both restricting access to individual resources through administrative procedures and designating materials and organisations as extremist through judicial proceedings.

In total, more than 6,300 internet resources have been designated as extremist in the country, and more than 18,000 have been blocked.

The powers of public authorities are further expanded through the adoption of new subordinate regulations. For example, in September 2025, a separate resolution of the Council of Ministers provided for the possibility of disconnecting individual subscribers from mobile communications and the internet.

The practice of restricting access to the internet or individual resources on a nationwide scale was applied during mass protests in August 2020 and during the presidential elections in January 2025. Unlike the near-complete internet shutdown in 2020, , the restrictions imposed in 2025 were more selective, manifesting as disruptions to access to individual platforms.

---

[1] Note: The website https://a1digital.by/ was not functioning at the moment of the conduct of the study.

According to some reports, DPI technologies were used during the 2020 blockages.

Despite the fact that information on the use of AI systems for internet censorship in Belarus is not publicly available, the scale and speed of blocking objectively suggest the use of automated monitoring and information-processing tools. At the same time, the absence of dedicated legal regulation enables government agencies to covertly deploy AI systems, making it difficult to assess the actual scale of its use.

Use of AI Systems for Overt and Covert Surveillance

The legal basis for the use of various surveillance systems by government agencies is set out in the Law "On Operational-Investigative Activities." In 2014, a presidential decree "On Issues of Creation and Application of a Video Surveillance System in the Interests of Public Order" was issued. It defines the responsible agencies and the procedure for equipment installation.

The central element of the video surveillance system in Belarus is the Kipod platform, developed by the Belarusian company Synesis. The platform is based on AI systems for monitoring offences and the movement of people and vehicles.

According to data from the Ministry of Internal Affairs, as of 2025, more than 60,000 cameras are operational in the country, connected to a unified platform using Kipod technologies.

In 2010, a presidential decree "On Measures to Improve the Use of the National Segment of the Internet" was issued. It regulates the installation of SORM infrastructure in accordance with the Russian model. The equipment's technical specifications were defined in 2023 in a separate document.

In December 2025, journalists reported the discovery of a previously unknown spyware called ResidentBat, used by Belarusian intelligence services to surveil journalists.

Georgia

Strategies and Legal Regulation

The National AI Development Strategy in Georgia is at the stage of development and discussion. General legislation applies to the AI sector.

In 2024, Georgia signed the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, under which states undertake obligations to mitigate risks to human rights, democracy, and the rule of law that may arise at all stages of the AI system lifecycle.[2] It is expected that further steps toward legal regulation will be aligned with the spirit of the CoE Convention and the EU approach.

Funding and Strategic Projects

AI sector funding is included in overall digital development expenditures. Direct funding is primarily channelled through startup support by the Georgia Innovation and Technology Agency (GITA), which has identified AI as one of the country's three key technological priorities. AI systems are being gradually deployed across sectors such as education, healthcare, and finance.

Use of AI Systems for Censorship

The Georgian National Communications Commission (ComCom) carries out the blocking of websites that violate the country's legislation (copyright infringement, gambling, pornography); however, a unified blacklist of prohibited content and internet resources is not maintained.

---

[2] Note: The Framework Convention has not yet entered into force, as it had not been ratified by the requisite number of states at the time of report preparation.

In general, the use of AI systems for content blocking is at an early stage; however, laws prohibiting LGBTQ+ propaganda, on foreign agents, and on insulting the authorities open up broad possibilities for content moderation.

In 2023, Meta removed a network of 117 accounts that had been posting information in support of the government and criticising the opposition during protests. Meta linked this network to Georgian government agencies.

Use of AI Systems for Overt and Covert Surveillance

In recent years, more than 4,000 “smart” cameras and other infrastructure from Japanese, Chinese, and Russian manufacturers (NEC, Hikvision, Dahua, and Papillon Systems) have been installed in Georgia.

In 2024, legislative amendments first introduced a ban on covering faces, using pyrotechnics, and lasers during public events. In 2025, biometric identification for locating persons who committed administrative offences was also legalised through legislative amendments. Nevertheless, the laws and subordinate regulations do not govern the procedural safeguards for the use of these technologies; this remains at the discretion of law enforcement agencies, with inadequate measures for public disclosure.

Human rights defenders note that cameras equipped with facial recognition technology were widely deployed during the 2024–2025 protests, resulting in fines for blocking streets totalling more than USD 730,000.

Kazakhstan

Strategies and Legal Regulation

The principal strategic document is the AI Development Concept for 2024–2029. The document identifies the need to adopt additional legal acts to ensure the safe and ethical use of new technologies. At the same time, certain AI-adjacent areas are planned to be regulated under the framework of the Concept for Digital Transformation, the Development of the Information and Communication Technologies Sector, and Cybersecurity for 2023–2029.

In early 2026, the Law "On Artificial Intelligence" entered into force, regulating relations in the field of AI system development and deployment. The Law establishes seven prohibited AI practices and further subdivides the remaining AI systems into three groups by risk level to the safety of users, society, and the state: high, medium, and minimal. Among the prohibited practices are:

- manipulation of vulnerabilities of specific social groups;
- social or biometric classification for discriminatory purposes;
- emotion recognition without consent;
- violations of personal data legislation;
- creation and dissemination of materials prohibited by law.

Requirements for the labelling of synthetic content are also introduced. At the same time, while the document adopts a risk-based approach similar to that of the EU AI Act, in its current form, it is more of a foundation that will be further detailed through secondary legislation. For example, requirements for users and operators of AI systems are identified. However, they are barely linked to the differentiation of AI systems by risk group.

To implement state policy, the Ministry of Artificial Intelligence and Digital Development was established in September 2025. Additionally, in mid-2026, a new Digital Code will enter into force, establishing comprehensive regulation for the information technology sector.

Funding and Strategic Projects

According to the AI Development Concept, 51 data centres are already operational in Kazakhstan, 15 of which belong to the e-government infrastructure operator. Additionally, several supercomputers of varying capacities are to be established at research institutions.

In March 2025, an agreement was signed with the Singaporean company GK Hyperscale Ltd to construct Tier 3 data centres. Investments totalling USD 1.5 billion were attracted.

In July 2025, the Kazakhstani company Akashi Data Centre and the Chinese telecommunications company China Mobile signed a memorandum of cooperation to create Central Asia's largest Tier 4 data centre.

In July 2025, the supercomputer centre Alem.cloud was launched in Astana. With a capacity of approximately 2 exaflops, it is the most powerful supercomputer in Central Asia,. The supercomputer was created in partnership with the UAE company Presight.

In 2024 and 2025, several AI models fine-tuned on Kazakh-language datasets were released based on Meta's Llama model: KazLLM and Sherkala (8B). Additionally, a proprietary large language model, AlemLLM and a multimodal model, Oylan, were developed. In 2025, a collaboration between Telegram and Kazakhstan's supercomputer cluster was announced to implement projects at the intersection of AI technologies and blockchain.

To develop the AI ecosystem, a National AI Platform was created, providing developers with access to high-quality data and computational resources within a secure government network, as well as the International AI Centre Alem.AI.

Use of AI Systems for Censorship

The legal basis for content and internet resource blocking is the Law of the Republic of Kazakhstan "On National Security," which allows government agencies to forcibly suspend telecommunications during counter-terrorism operations or the suppression of mass disturbances.

Article 41-1 of the Law "On Communications" establishes an administrative procedure for the temporary suspension of communications and blocking of internet resources. Upon a submission by the Prosecutor General or their deputies, or by an urgent decision of national security agencies, telecommunications operators, online platforms, and the state technical service are required to restrict the operation of networks, communication services, or access to content used for criminal purposes within two hours. Prior judicial authorisation is not required in such cases; notification of the restriction is provided post factum. Once the violation is remedied, the restrictions may be lifted.

Within the framework of these powers, the Cybernadzor (Cyber Supervision) project was launched in 2017 as an information system through which government agencies interact to identify and block unlawful content. Using this information system, hundreds of thousands of internet links have been blocked, as have more than 38,000 internet resources containing unlawful content. Although the use of AI systems in the operation of this information system is not explicitly stated, the volume of blocked information suggests that automated solutions may be deployed.

Under the Law "On Countering Extremism," prosecutorial oversight may be exercised over the dissemination of prohibited information, and an organisation may be designated as extremist by court order. Similar measures are also carried out under the Law "On Countering Terrorism."

In accordance with Article 14 of the Law "On Online Platforms and Online Advertising," the owner or legal representative of an online platform is required to remove unlawful content or false information about an individual.

During mass protests in January 2022, internet shutdowns and messenger blockages were observed for a week.

Use of AI Systems for Overt and Covert Surveillance

Video surveillance in public places is conducted pursuant to the Law "On Operational-Investigative Activities." However, the use of AI systems is not separately regulated by legal acts, except for the prohibited practices introduced by the Law "On Artificial Intelligence."

According to data as of 2025, the overall video surveillance network comprises more than 1.6 million cameras. Of these, 475,000 are connected to Operational Command Centres, and 20,500 to AI systems. The majority of the infrastructure uses equipment from Chinese manufacturers Hikvision and Dahua Technology. Kazakhstan is also developing its own surveillance systems, such as the AI platform TargetEYE.

Article 48 of the Digital Code provides for the creation of a national biometric authentication system, which will become the key instrument for accessing public services, conducting verification, and protecting personal data. The requirement for citizens to submit their biometric data is gradually expanding across various services. For example, since January 2026, SIM cards in the country can be purchased only after submitting biometric data. The existence of a centralised data storage facility in the hands of government agencies potentially creates extensive opportunities for real-time AI-powered surveillance.

According to journalists, during the 2022 protests, China dispatched a special video analytics team to Kazakhstan to identify protesters using AI systems.

The country also uses SORM infrastructure with deep packet inspection (DPI) technology. According to journalists, Kazakhstan previously used Russian technologies, but in recent years they have been replaced by systems and software from Chinese companies (e.g., Geedge).

Kyrgyzstan

Strategies and Legal Regulation

In September 2025, information emerged that a future AI Development Concept is being developed and discussed in the country. It aims to define the strategic objectives for the sector's development.

In early 2025, a National AI Development Council was established as an advisory body to facilitate interaction among various stakeholders.

Since 2026, the Digital Code has been in effect as a comprehensive legal framework aimed at regulating relations in the information technology sector. Article 16 of the Code provides the president with the power to introduce "special regulation," which may subsequently be used as a legal justification for the implementation of repressive and restrictive measures, including on the internet.

Chapter 23 of the Code directly addresses the development and deployment of AI systems, including requirements for developers and users of high-risk AI systems and disclosure requirements. Although these provisions are conceptually similar to the requirements for operators of high-risk AI systems under the EU AI Act, their implementation will largely be determined by secondary legislation.

Funding and Strategic Projects

In 2025, the procurement of data centre equipment worth USD 2.5 million was announced to complement the existing infrastructure.

According to media reports, the AkylAI (Akylai) AI assistant project has been under development since 2023 and is architecturally based on Meta's

Llama model, trained on a Kyrgyz-language dataset.[3] It was also announced that a smart speaker would be created as part of the project.

Use of AI Systems for Censorship

Content and internet resource blocking through judicial proceedings is carried out in accordance with Chapter 25 of the Civil Procedure Code, which establishes the procedure for restricting access to terrorist or extremist materials. The concept of such materials and restrictions on their dissemination are defined by the Law "On Countering Extremist Activities". A separate blacklist of content or internet resources has not been published. However, lists of resources blocked by court order can be found on operator websites. For example, the list maintained by the Megaline operator contains more than 200 entries.

In 2021, the Law of the Kyrgyz Republic "On Protection from False Information" was adopted, granting private individuals the right to demand the removal of online content about themselves they consider false within 24 hours, under threat of website suspension. According to human rights defenders, this law is also used as an extrajudicial means of content removal and restricting access to internet resources.

In April 2024, access to TikTok was blocked. The official reason was non-compliance with the Law "On Measures to Prevent Harm to Children's Health, Their Physical, Intellectual, Mental, Spiritual, and Moral Development," adopted in August 2023. Human rights defenders warn that this law may be used as grounds for blocking.

According to journalists, "troll factories" were used during the 2020 parliamentary elections. In 2024, amendments to the Law "On Non-Commercial Organizations" were adopted, adding provisions modelled on Russia's foreign agents legislation.

Despite the fact that there is currently no information on the use of AI systems to restrict access to content and internet resources, government

---

[3] Note: The website https://www.akylai.com/ was not functioning at the moment of the conduct of the study.

agencies have the necessary legal mechanisms to deploy them without adequate transparency requirements.

Use of AI Systems for Overt and Covert Surveillance

The legal basis for video surveillance is the Law “On Operational-Investigative Activities” and the Law “On Personal Data”. No separate provisions on the processing of biometric data are contained even in the new Digital Code.

As of 2025, the Ministry of Internal Affairs reports the connection of approximately 25,000 video cameras within the “Safe Country” project, including cameras from other agencies, some of which use facial recognition and are integrated with MIA databases. Previously, approximately 12,000 cameras were installed as part of the “Safe City” project. The exact technical specifications of the infrastructure have not been publicly disclosed. In the early stages of building the surveillance system, cooperation was conducted with Chinese companies CEIEC and Huawei, as well as the Russian company Vega.

In 2014, a government resolution was adopted establishing the procedure for interaction between mobile operators and law enforcement agencies. In effect, the document provides the legal basis for the installation of SORM infrastructure in accordance with the Russian model.

Russia

Strategies and Legal Regulation

The principal strategic document is the National AI Development Strategy to 2030. The Strategy was approved by presidential decree and serves as a programmatic document. A comprehensive system of legal regulation has not been developed in the country. Current regulation covers only specific sectors, such as data circulation, medicine, and transport.

Experimental legal regimes (ELRs), the rules for which are established by federal law, were long considered the key regulatory instrument. A separate experimental regime, aimed primarily at facilitating simplified access to citizens' data, has been operational in Moscow since 2020.

Technical Committee No.164 actively develops its own standards and adapts international standards in AI, most of which are advisory in nature.

The principal focus is on the AI Ethics Code and supplementary documents. The document is voluntary and does not contain specific obligations for actors, which allows it to create a "facade" of regulatory governance in the substantive absence thereof. Russia also actively promotes this code beyond its borders.

Funding and Strategic Projects

The Strategy stipulates that by 2030, computing capacity should increase to at least 1 exaflop, up from 0.073 in 2022. Organisational expenditures on the deployment and use of AI technologies should increase to at least RUB 850 billion per year, up from RUB 123 billion in 2022.

Within the national project "Data Economy and Digital Transformation of the State," the federal project "Artificial Intelligence" is being implemented. Total expenditures for 2025–2027 will exceed RUB 26 billion. The entire

national project through 2030 is estimated at RUB 1–1.5 trillion, excluding private investment in the sector's development.

The country's political leadership actively proclaims a course toward creating "sovereign" AI models, whose outputs must comply with legislation and "traditional values." To date, Russia has two principal AI models: YandexGPT and GigaChat. Both have been developed by state-affiliated companies Yandex and Sber (the largest Russian bank). Other private companies are either developing their own AI models or using Chinese models (Qwen, DeepSeek, Kimi, etc.). Nevertheless, the development of sovereign models is hampered by stringent Western sanctions that restrict the supply of chips, cloud resources, and models, as well as by insufficient funding and personnel amid the war in Ukraine. Equipment supplies are typically carried out illegally with the participation of countries friendly to Russia.

Use of AI Systems for Censorship

Over the past several decades, Russia has been gradually building a system of total state control over the internet. The principal act determining the procedure for restricting access to information is the Law "On Information, Information Technologies, and Protection of Information." The document establishes extrajudicial and judicial procedures for the inclusion of network addresses and domain names in a unified registry. After a resource is included in the registry, website owners, hosting providers, and telecommunications operators must take the necessary measures to remove the content. According to information as of early 2026, the registry contains more than 4.7 million entries.

In the practice of implementing blockages in Russia, the automated system "Revizor" is used, developed by Roskomnadzor and designed to monitor telecommunications operators' compliance with requirements to restrict access to prohibited information.

Following the adoption of the so-called "sovereign Runet" law, which introduced amendments to the Law "On Information..." and the Law "On Communications," telecommunications operators became obligated to install Technical Means of Countering Threats (TSPU) with deep packet

inspection (DPI) technology. This enabled mass blocking of social networks, digital platforms, and VPN services after 2022. Since 2024, following the implementation of the "Mir" information system, website monitoring has been carried out by government agencies using AI systems.

In the architecture of the "sovereign Runet", a key role is played by the Centre for Monitoring and Management of the Public Communications Network (CMU SSOP) and the eponymous information system for monitoring and managing the public communications network, which together provide a centralised infrastructure for surveillance and network management.

Since 2023, the "Oculus" information system has been used for the automated identification of prohibited content on the internet. In 2024, information emerged about the registration of the "Vepr" information system for internet monitoring. Additionally, the AS "Mavr" system was launched to identify unlawful content on streaming services.

Russia also actively uses AI systems for disinformation. In July 2024, the U.S. Department of Justice announced the disruption of an AI-powered bot farm that created fictitious profiles of Americans on social networks and disseminated pro-Kremlin narratives. Deepfakes were mass-produced in the context of the war in Ukraine and the U.S. presidential elections. Russian propaganda materials are extensively infiltrating the training datasets of advanced AI models (ChatGPT-4, Grok, Mistral, Copilot, Meta AI, Claude, Google Gemini, etc.), affecting the content of their outputs.

Use of AI Systems for Overt and Covert Surveillance

The principal document vesting government agencies with surveillance powers is the Law "On Operational-Investigative Activities." According to the Ministry of Digital Development data, more than 1 million cameras are operational in Russia. The largest network operates in Moscow. It is integrated with the government information system "Unified Centre for Data Storage and Processing (UCHSD)." Since 2020, an experiment aimed at developing AI technologies has been implemented in Moscow, facilitating

the unrestricted collection of personal data without the subject's consent, in accordance with a separate federal law. The principal suppliers of surveillance equipment and software are NtechLab, Tevian, VisionLabs, and Belarus Kipod. Within the national project “Data Economy and Digital Transformation of the State,” it is projected that by 2030, the number of video surveillance cameras in the country will increase to 5 million, all of which will be integrated into a unified information system and equipped with AI systems for video stream processing.

It is important to note that the use of AI systems and other digital technologies for overt and covert surveillance is not supported by a legal framework and is effectively arbitrary for government agencies, which was specifically noted in the ECtHR judgment in the case of Glukhin v. Russia.

For identification and authentication, the Unified Biometric System, which stores all biometric data, was created in 2018. . It is expected that in the future, the biometric data of all persons present on the territory of the Russian Federation will be stored in the database. Thus, the state has both exclusive access to all biometric data and the ability to determine which actors will be granted access to the database.

In 2024, under the pretext of creating a mechanism for exchanging datasets to enable businesses to develop AI systems, amendments (Article 13.1) were introduced into the Law “On Personal Data,” providing for the creation of a unified state system for storing such data.

Since 1996, SORM infrastructure has been gradually deployed, enabling comprehensive processing and storage of all information from social networks, messengers, and telephone conversations. In 2014–2015, deep packet inspection (DPI) technologies began to be integrated into SORM.

In 2025, in parallel with the blocking of popular messengers and social networks by government agencies, the pro-government messenger “MAX” was introduced.

Tajikistan

Strategies and Legal Regulation

The principal strategic document is the AI Development Strategy to 2040. Tajikistan became the first country in Central Asia to adopt a national AI strategy. The Strategy identifies key areas for the integration of AI into various spheres of public life and, as one of its goals, sets out the development of a regulatory framework, including the creation of dedicated legislation and updates to existing law.

To implement the Strategy, an Interagency Commission on AI Regulation was established under the Agency for Innovation and Digital Technologies under the President of the Republic of Tajikistan.

In 2025, on Tajikistan's initiative, the UN General Assembly unanimously adopted the resolution "The Role of Artificial Intelligence in Creating New Opportunities for Sustainable Development in Central Asia," which provides for the establishment of a Regional AI Centre in Dushanbe.

Funding and Strategic Projects

In October 2025, the AI Conf 2025 conference was held in Dushanbe, with participants from more than 20 countries. Within the framework of the conference, a number of projects were announced:

- the creation of a dedicated AI Zone, whose members will include local startups and international companies;
- the launch of the Soro project in cooperation with UNICEF and the startup zypl.ai for the integration of AI systems into the education sector;
- the announcement of SoroLLM an AI model built on Tajik-language datasets;

- the announcement that darya.ai and Indian company Yotta Data Services signed a cooperation agreement for the creation of an eco-friendly AI data centre.

In addition, government agencies have concluded cooperation agreements with Huawei, Perplexity AI, Google DeepMind, NVIDIA, Presight, and Scale AI. Furthermore, zypl.ai, one of the country's key startups in credit scoring, is being actively deployed across government agencies and banks.

Use of AI Systems for Censorship

Since late 2015, the Unified Electronic Communications Switching Centre (UECSC), established by a government resolution, has served as the primary element of traffic control in the country. This document requires all telecommunications operators and internet service providers to route all international traffic through a state gateway managed by Tojiktelecom. Although individual operators were allowed purchase international traffic directly in 2023, in 2025, a unified national internet exchange point (TJ-IX) was launched on the Tojiktelecom platform.

The powers of agencies to block content and internet resources are not explicitly prescribed by law but derive from the general requirements of the laws "On Information," "On Mass Media," and the "Rules for the Provision of Internet Services." Public authorities block resources through administrative procedure; the blacklist is not publicly available. It is known that Asia-Plus and Radio Ozodi (Radio Liberty) are blocked.

The laws "On Countering Terrorism," "On Countering Extremism," and "On the State of Emergency" are also used as grounds for restricting internet access. For example, following the forceful suppression of protests in the Gorno-Badakhshan Autonomous Region, a 4-month internet blackout was imposed.

In 2018, parliament criminalised the use of "like" and "repost" functions on social networks in relation to content associated with terrorism and extremism, with a maximum penalty of up to 15 years of imprisonment (Article 179(3) of the Criminal Code). In May 2025, a law entered into force

abolishing criminal liability for “likes”; however, by that time, more than 1,500 persons had been convicted..

Despite the absence of direct evidence of AI system use for internet space control, the existence of the legislative framework makes this question purely technical.

Use of AI Systems for Overt and Covert Surveillance

The use of video surveillance and biometric identification technologies occurs in the absence of dedicated legal regulation. The legal basis is the Law “On Operational-Investigative Activities.” The urban video surveillance system has been developing within the “Safe City” project since 2013, with the gradual installation of additional cameras in major population centres. The AI Development Strategy also provides for integrating video surveillance with intelligent analytics systems, including automated analysis of traffic and urban flows. According to open-source data, equipment from Chinese manufacturers (Huawei) is being installed.

Since 2001, telecommunications operators have been required to install SORM technical facilities. As of 2023, the country operates SORM-1 (telephony) and SORM-2 (internet) systems.

In November 2025, Tojiktelecom launched the national messenger Oriz with servers located exclusively within the country’s territory. In essence, it resembles the Russian messenger MAX and the Kazakhstani Aitu.

Uzbekistan

Strategies and Legal Regulation

The foundational strategic document is the AI Technology Development Strategy to 2030. The Strategy envisages the broad deployment of AI systems across all spheres of public and state activity, as well as the development of comprehensive legal regulation. Implementation is divided into three phases: infrastructure creation (2024–2025), scaling (2026–2028), and commercialisation (2028–2030).

In November 2025, the Senate approved a draft law amending several regulatory acts governing relations arising from the deployment of AI systems.[4]

An important element of regulation is also the data localisation requirement within Uzbekistan's territory, established by Article 27[1] of the Law "On Personal Data".

In December 2024, draft ethical rules for the development and deployment of AI systems were published.

Funding and Strategic Projects

Infrastructure for the development of digital innovations in the country was initially created in 2019 as part of the IT Park Uzbekistan project.

The Strategy provides for the allocation, starting January 1, 2025, of an interest-free USD 50 million loan to the Ministry of Digital Technologies for

---

[4] At the moment of the conduct of the study, the document had not been published; however, based on press releases, it can be concluded that it will be aimed at defining terminology, establishing rules for the use of specific AI systems, and clarifying the specifics of personal data processing.

a 5-year term, including a 2-year grace period, for the development of AI technologies.

Additionally, by presidential decree, USD 100 million was allocated for 2026–2027 to finance projects, including startups in the social sphere and in AI-related economic sectors.

In 2025, the commencement of a new infrastructure project in partnership with the Saudi company DataVolt was announced. It concerns the construction of data centres with a total capacity of up to 500 MW and a cost of USD 5 billion by 2030.

Use of AI Systems for Censorship

The Information Space Monitoring Centre of Uzkomnazorat, in coordination with other agencies,identifies and ensures the removal of unlawful information through extrajudicial procedure. The unified registry is not publicly available.

Through judicial procedure,extremist and terrorist materials may be blocked on the basis of decisions by courts of general jurisdiction made upon submission by authorised law enforcement agencies. Lists of materials designated as extremist/terrorist are regularly published on the Supreme Court website and in the media. The latest version of the list contains more than 1,600 resources.

The internal activities of public authorities are opaque, making it impossible to conclude with sufficient certainty whether AI systems are being used by government agencies to identify unlawful content.

A precedent of a complete internet shutdown occurred in June–July 2022 in Karakalpakstan during protests against restrictions on regional autonomy.

Use of AI Systems for Overt and Covert Surveillance

In April 2019, Huawei signed a contract worth USD 1 billion to deploy a Safe City system with 883 cameras in Tashkent.

Within the framework of the state program for digitisation and AI deployment, a decision was made to pilot the UzFace facial recognition system. According to a Cabinet of Ministers resolution, the project is planned to be launched at entrances to Tashkent railway stations in 2025–2026 as part of the priority initiatives for AI development. Previously, government structures also considered the expanded use of biometric technologies, including facial and fingerprint recognition, for law enforcement purposes, while Face-ID technology has been incorporated into government identification services via Mobile-ID.

Since 2006, all telecommunications operators have been required, pursuant to Article 18 of the Law “On Telecommunications,” to install SORM-compatible equipment.

Conclusions

1. Countries in the region demonstrate significant heterogeneity in their approaches to regulatory oversight of AI. Based on the degree of development of specialised legislation, three groups can be identified:

- **Countries with a comprehensive approach to regulation:** Kazakhstan adopted a special law "On Artificial Intelligence" (2025), and Kyrgyzstan has integrated a chapter on AI systems into its Digital Code (2026). Despite the similarity of certain elements of these regulations to the EU AI Act, these laws are more of a starting point for regulation, brought to the level of secondary legislation. This creates uncertainty regarding human rights protection and poses significant risks to fundamental rights, including the right to privacy and freedom of information.
- **Countries with a conceptual approach to regulation:** Russia, Uzbekistan, Tajikistan, and Azerbaijan, have adopted strategic documents and concepts for AI development, but comprehensive legislation is still in the drafting stage. A characteristic feature is the use of "soft law" instruments (codes of ethics, voluntary standards), which create the appearance of regulatory activity in the absence of binding norms.
- **Countries with an undeveloped approach to regulation:** Armenia, Georgia and Belarus have neither specific legislation nor detailed conceptual documents in the field of AI. General legislation applies to AI in these countries.

2. In states with authoritarian tendencies, the development of AI regulation is primarily aimed at legitimising the use of surveillance technologies rather than protecting human rights. Prohibitions on certain AI practices (manipulative methods, discriminatory classification) and risk-based restrictions, formally included in the legislation of Kazakhstan and Kyrgyzstan, do not apply to law enforcement activities or contain exceptions for national security purposes.

At the same time, legislation on countering extremism and terrorism in all the countries studied contains broad, vague wording that allows arbitrary interpretation and creates a legal basis for restricting freedom of expression and the right to privacy, including through state-level AI systems that automate decision-making.

3. China and Russia actively export repressive technologies to Eurasian countries. Equipment from Huawei, Hikvision, and Dahua is installed in all of the countries studied. The Safe City and Smart City projects in Kazakhstan, Uzbekistan, Tajikistan, Kyrgyzstan, and partially in other countries have been implemented using Chinese technologies.

The Russian SORM infrastructure has been implemented in various countries studied, with the exception of Georgia. The system allows for the interception of telephone calls and internet traffic without effective judicial oversight.

Diversification of partners is characteristic of Armenia (reorientation towards the United States and India), Tajikistan (cooperation with India, the UAE, and Western technology companies), and, to a lesser extent, Kazakhstan (partnership with the UAE and Singapore). However, this diversification mainly concerns computing infrastructure and language model development, while surveillance systems remain largely dependent on Chinese and Russian technologies.

4. All the countries studied possess the legal and technical capabilities to restrict access to internet content. The following models can be conditionally identified:

- **Centralised model with AI system deployment (Russia):** a developed ecosystem of automated solutions (“Revizor,” “Oculus,” “Vepr,” “Mir,” AS “Mavr,” etc.) operates, ensuring the real-time identification and blocking of content. The installation of TSPU with deep packet inspection (DPI) capabilities enables protocol-level blocking.
- **Centralised model with early-stage or unconfirmed AI system deployment (Azerbaijan, Belarus, Kyrgyzstan, Tajikistan):** all international traffic is routed through state nodes, enabling a complete

internet shutdown. The use of AI systems is not documented; however, the scale of blockages (more than 18,000 resources in Belarus) suggests the use of automated tools, including AI-based ones.

- **Decentralised model (Armenia, Georgia):** blocking is targeted and carried out predominantly against content that violates legislation (gambling, pornography, copyright infringement). At the same time, in Georgia, an expansion of grounds for blocking is noted (laws on "LGBTQ+ propaganda," on foreign agents).

5. Biometric identification systems using facial recognition technologies have been deployed or are being deployed in all the countries studied. The most advanced systems operate in Russia (more than 1 million cameras, the Unified Biometric System, and a combination of AI systems from several vendors), Belarus (Kipod platform, more than 60,000 cameras), and Kazakhstan (more than 1.6 million cameras, of which 20,500 are integrated with AI systems).

A characteristic trend is the post-hoc legalisation of biometric identification: technologies are first deployed, and then legislation legitimising their use is adopted. At the same time, such legislation generally does not include procedural safeguards, independent oversight mechanisms, or other means to ensure public transparency.

6. The development of "sovereign" AI models, positioned as instruments of technological independence, creates unprecedented risks to human rights.

Russia openly declares a course toward creating models aligned with "traditional values" and state interests. The YandexGPT and GigaChat models operate with built-in restrictions on generating content that contradicts state policy. Similar trends are observed in Kazakhstan (KazLLM, AlemLLM), Kyrgyzstan (AkylAI), and Tajikistan (SoroLLM).

The proliferation of "sovereign" AI models gives rise to several groups of risks:

- Models trained on controlled datasets can systematically distort information about politically sensitive topics, creating an alternative

informational reality that the user perceives as objective. Russia demonstrates advanced practices in deploying modern AI models for disinformation: AI-powered bot farms, the mass generation of deepfakes, and the targeted “poisoning” of training datasets for foreign AI models (ChatGPT, Claude, Gemini, etc.) with propaganda materials.

- The integration of advanced AI models with monitoring systems enables automated identification of content that previously required active human involvement. This radically expands the scope of censorship. The combination of advanced AI models with centralised citizen data collection enables the personalisation of propaganda and opens up possibilities for the preventive identification of “unreliable” individuals.
- The availability of open-source AI models (Llama, DeepSeek, etc.) that developers can fine-tune without restrictions will enable the creation of adapted models with minimal resources for subsequent integration into the repressive infrastructure of authoritarian states.

Dmitry Kuteynikov and Sergey Kuznetsov for RKS Global