MEMORIAL

HUMAN RIGHTS DEFENCE CENTRE

ON NEW METHODS, REGULATIONS, AND TECHNOLOGIES FOR SURVEILLANCE OF FOREIGN CITIZENS IN THE RUSSIAN FEDERATION

Report by the Analytical Unit of the “Migration and Law” Network

Prepared by Konstantin Troitskiy

Content

Introduction

Surveillance practices have been an integral part of human history.[1] However, whereas surveillance was once severely limited, the advent of new technologies and the transition to digital formats—enabling the transmission, accumulation, storage, and analysis of diverse data—have elevated surveillance to an unprecedented level of scope, depth, and complexity. This development has led some researchers to distinguish between "traditional surveillance," which relies on direct visual or auditory contact and rudimentary recording tools, and "new surveillance," which is based on advanced digital technologies.[2]

Surveillance is an ambivalent and multifaceted phenomenon conducted for various purposes by a wide range of actors, including banks and telecom operators, media outlets and lawyers, medical institutions and sports clubs, airports and hotels, educational institutions and charitable foundations, research centers and factories, criminals and investigators, transport services and construction workers, municipalities and government agencies, internet platforms, and messaging apps, among others. In developed societies, aided by new technologies: (a) everyone is subject to surveillance through government records, internet trackers, video cameras, satellites, identification and registration systems, medical tests, and more; (b) many individuals surveil each other using mobile apps, photo and video recording, drones, social media, and similar tools; and (c) some engage in self-surveillance via mobile apps, electronic diaries, smartwatches, and related devices.[3]

When adopting a human rights perspective, the primary questions are not whether to permit surveillance, but rather on what principles it is based—that is, what purpose it serves, how it is conducted, and whether there is independent public oversight of its implementation. This is especially relevant to state surveillance, which has become a recurring topic in many UN bodies.[4] Human rights and expert organizations have also formulated principles that states should follow when implementing and using surveillance technologies.[5] It is one thing for state surveillance to aim to protect fundamental human rights and freedoms, to be conducted in accordance with clear norms, and to be monitored by independent human rights and expert organizations. It is quite another when surveillance is used to consolidate and maintain power, lacks regulation, and there is no independent human rights oversight. In the latter case, we are dealing with authoritarian regimes. When such regimes rely heavily on digital technologies to maintain and strengthen their power, suppressing protests and persecuting dissidents, researchers refer to this phenomenon as digital

---

[1] Toni Weller, "The historical ubiquity of surveillance," *Histories of Surveillance from Antiquity to the Digital Era,* edited by Andreas Marklund and Laura Skouvig (Routledge, 2022), 175.
[2] Gary Marx, *Windows into the Soul. Surveillance and Society in an Age of High Technology* (The University of Chicago Press, 2016), 15–18.
[3] A brief introduction to the phenomenon of "surveillance," highlighting its diversity, complexity, and ambivalence, is provided here: David Lyon, *Surveillance* (Oxford, Oxford University Press, 2024).
[4] See e.g., United Nations Human Rights Council. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression: "Surveillance and Human Rights". *United Nations Human Rights Council*, 2019, https://digitallibrary.un.org/record/3814512?ln=en&v=pdf [accessed October 15, 2025] and United Nations Human Rights Council. Report of the Office of the United Nations High Commissioner for Human Rights: "The Right to Privacy in the Digital Age". *United Nations Human Rights Council*, 2022, https://docs.un.org/en/A/HRC/51/17 [accessed October 13, 2025].
[5] See e.g., Access, EFF, Privacy International, et. al. "The International Principles on the Application of Human Rights to Communications Surveillance," https://necessaryandproportionate.org/principles/ [accessed November 21, 2025].

authoritarianism;[6] when they actively engage with the latest technologies, including those based on artificial intelligence, it is termed algorithmic authoritarianism.[7]

In authoritarian regimes, surveillance systems assume an all-encompassing role, becoming integral components of the repressive apparatus. These regimes employ surveillance to monitor all significant social, cultural, economic, and political processes. Surveillance also enhances the effectiveness of mass propaganda and disinformation campaigns and is used, either directly or indirectly, to suppress opposition.[8] The development of new technologies and close cooperation among authoritarian regimes further increase the effectiveness of these surveillance systems. This collaboration enables them to exchange technologies, share data and practices, circumvent sanctions, coordinate disinformation campaigns, and synchronize repressive actions.[9] Of particular concern to experts and human rights activists is the growing use of artificial intelligence technologies by authoritarian regimes for surveillance, aggression, and repression.[10]

In what follows, I will use the following definition: state surveillance is any routine, mass, focused, and systematic monitoring by state bodies and their affiliated agents of personal data and behavior for the purposes of governance, protection, control, and—in the case of authoritarian regimes—repression of political opponents, independent journalists, and social activists.[11]

The history of surveillance in Russia spans centuries but became systematic and large-scale with the establishment of a strong centralized state. By the late 19th and early 20th centuries, the Russian Empire had developed a surveillance network featuring increasingly sophisticated record-keeping systems, as well as informants, provocateurs, and denunciators.[12] However, this was overshadowed by the Soviet surveillance apparatus, which became a tool of repression that, during the Stalin era, reached a scale, complexity, and cruelty unprecedented in human history.[13] In the late 1980s and early 1990s, surveillance in the USSR and later in the Russian Federation underwent a period of "perestroika" and decline, raising hopes for the creation of a modern state surveillance system grounded in respect for human rights and subject to public oversight. These hopes, however, were not realized. By the early 2000s, Russian authorities began constructing a new authoritarian state

---

[6] See e.g., James S. Pearson, "Defining Digital Authoritarianism," *Philosophy & Technology* 37, no. 73 (2024), https://link.springer.com/article/10.1007/s13347-024-00754-8#Fn2 [accessed October 4, 2025].

[7] See e.g., Akin Ünver, *Artificial intelligence (AI) and human rights: Using AI as a weapon of repression and its impact on human rights* (European Union, Directorate General for External Policies of the Union, 2024), https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2024)754450 [accessed November 21, 2025].

[8] Steven Feldstein, *The Rise of Digital Repression. How Technology Is Reshaping Power, Politics, and Resistance* (Oxford University Press, 2021); Minxin Pei, *The Sentinel State. Surveillance and the Survival of Dictatorship in China* (Harvard University Press, 2024); Anita R. Gohdes, *Repression in the Digital Age. Surveillance, Censorship, and the Dynamics of State Violence* (Oxford University Press, 2024).

[9] See e.g., Anna Applebaum, *Autocracy, INC. The Dictators Who Want to Run the World* (Doubleday, 2024).

[10] See e.g., Ünver, *Artificial intelligence (AI) and human rights: Using AI as a weapon of repression and its impact on human rights,* https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2024)754450 [accessed November 21, 2025].

[11] The definition of surveillance is derived from, but not reducible to, the definition proposed in Lyon, *Surveillance*.

[12] See e.g., Fredric S. Zuckerman, *The Tsarist Secret Police in Russian Society, 1880–1917* (New York University Press, 1996).

[13] On the relationship between surveillance and repression in the USSR during the Stalin period, see e.g., David R. Shearer, *Stalin's Socialism. Repression and Social Order in the Soviet Union, 1924-1953* (Yale University Press, 2009).

centered on special services that were unaccountable to society and obsessed with total surveillance and control.[14]

The rise of authoritarian tendencies in Russia in the early 2000s coincided with the emergence of unprecedented surveillance technologies.[15] Utilizing these technologies, Russian authorities began actively constructing a new surveillance system comprising sophisticated databases, networks of video cameras, internet monitoring, banking supervision, analytical centers, and research facilities.[16] This process accelerated after Russian authorities occupied Crimea and intensified further after Russian authorities unleashed open war against Ukraine in February 2024. The surveillance system was supported by the enactment of new repressive regulations. Since the late 2010s, this surveillance apparatus has been employed not only to record crimes and identify suspects but also to persecute political opposition, dissenting journalists, human rights defenders, and civil activists. Russian authorities have consistently disregarded the United Nations Human Rights Council's recommendations regarding the use of technology.[17] The surveillance system they have established fails to comply with international legal standards and is used for repressive purposes, as documented repeatedly by journalists,[18] researchers,[19] human rights organizations,[20] and the United

---

[14] See e.g., Andrei Soldatov and Irina Borogan, *The New Nobility: The Restoration of Russia's Security State and the Enduring Legacy of the KGB* (PublicAffairs, 2011).

[15] For information on new surveillance technologies that emerged at the turn of the 20th and 21st centuries, see e.g., Julie K. Petersen, *Introduction to Surveillance Studies* (Taylor & Francis Group, 2013).

[16] Anastassiya Mahon and Scott Walker, "Russia's Digital Repression Landscape: Unraveling the Kremlin's Digital Repression Tactics." *Journal of Illiberalism Studie*s 4 no. 3 (2024): 29–50; IPHR and Global Diligence. *Russia's Digital Authoritarianism: the Kremlin's Toolkit.* International Partnership for Human Rights (IPHR) and Global Diligence LLP, 2023, https://iphronline.org/articles/russias-digital-authoritarianism-the-kremlins-toolkit/ [accessed November 22, 2025].

[17] E.g., United Nations Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression: "Surveillance and Human Rights". *United Nations Human Rights Council,* 2019, https://digitallibrary.un.org/record/3814512?ln=en&v=pdf [accessed October 15, 2025]; United Nations Human Rights Council, Report of the Office of the United Nations High Commissioner for Human Rights: "The Right to Privacy in the Digital Age". *United Nations Human Rights Council*, 2022, https://docs.un.org/en/A/HRC/51/17 [accessed October 13, 2025]. United Nations Human Rights Council, Report of the Office of the United Nations High Commissioner for Human Rights: "Human Rights and New and Emerging Digital Technologies". *United Nations Human Rights Council*, 2024, https://docs.un.org/en/A/HRC/56/45 [accessed October 13, 2025].

[18] Krolik, Aaron, Paul Mozur, and Adam Satariano, "Cracking Dow,n on Dissent, Russia Seeds a Surveillance Supply Chain," *The New York Times*, July 3, 2023, https://www.nytimes.com/2023/07/03/technology/russia-ukraine-surveillance-tech.html [accessed August 19, 2025]; Evgeny Legalov, "Небольшой брат. Как видеокамеры стали инструментом репрессий" [A Little Brother: How Video Cameras Became a Tool of Repression]. *Radio Svoboda*, May 7, 2024, https://www.svoboda.org/a/neboljshoy-brat-kak-videokamery-stali-instrumentom-repressiy/32932369.html [accessed September 8, 2025].

[19] Tetyana Lokot, "Be Safe or Be Seen? How Russian Activists Negotiate Visibility and Security in Online Resistance Practices," *Surveillance & Society* 16, no. 3 (2018): 332–46; Rashid Gabdulhakov, "(Con)trolling the Web: Social Media User Arrests, State-Supported Vigilantism and Citizen Counter-Forces in Russia," *Global Crime* 21 no. 3–4 (2020): 283–305; Applebaum, *Auticracy, INC. The Dictators Who Want to Run the World*; Tatiana Lysova, "Paradoxes of Authoritarian Mundane Surveillance: The Use of the Yandex.Eda Data Leak to Investigate the Powerful in Russia," *Surveillance & Society* 23, no. 3 (2025): 321–35.

[20] OVD-Info, "Как власти используют камеры и распознавание лиц против протестующих" [How Russian Authorities Are Using Cameras and Facial Recognition Against Protesters]. *OVD-Info*, February 17, 2022, https://reports.ovd.info/kak-vlasti-ispolzuyut-kamery-i-raspoznavanie-lic-protiv-protestuyushchih [accessed September 25, 2025]; IPHR and Global Diligence. *Russia's Digital Authoritarianism: the Kremlin's Toolkit.* International Partnership for Human Rights (IPHR) and Global Diligence LLP, 2023, https://iphronline.org/articles/russias-digital-authoritarianism-the-kremlins-toolkit/ [accessed November 22, 2025]; OVD-Info and Roskomsvoboda, "Human Rights and New Technology in Russia," *OVD-Info and Roskomsvoboda,* March 6, 2023, https://ovd.info/en/human-rights-and-new-technology-russia?utm_source=google.com&utm_medium=organic&utm_term=%28not+set%29#1-6 [accessed November 25, 2025]; HRW, *Disrupted, Throttled, and Blocked State Censorship,*

Nations Human Rights Committee.[21] These surveillance practices have also been condemned several times by the European Court of Human Rights in cases such as Zakharov v. Russia, Glukhin v. Russia, and Podchasov v. Russia.

Foreign citizens in Russia[22] have long been the focus of special attention from Russian law enforcement agencies. Central Asian labor migrants and asylum seekers are particularly vulnerable in Russia, often becoming victims of xenophobia, systemic discrimination, and police brutality—issues that have intensified since the launch of the anti-migrant campaign in March 2024.[23] In recent years, Russian authorities have generally failed to formally acknowledge the need to protect migrants' rights. For instance, the "Concept of the State Migration Policy of the Russian Federation for 2019–2025"[24] addresses demographics, economics, security, and control but does not mention the protection of human rights. Labor migration is portrayed as a forced measure fraught with risks, necessitating the strictest monitoring and control. Consequently, Russian authorities have sought and developed new technological methods to track migrants more actively.

This trend accelerated in the 2020s, with 2024 and 2025 marking a turning point. In addition to expanding and enhancing existing surveillance methods—such as questionnaires, facial biometrics, fingerprints, linking SIM cards to specific users, video surveillance systems, internet monitoring, and wiretapping—several new techniques were introduced within a short period for all or key categories of migrants. These include voice biometrics, geolocation data collection, installation of user-tracking apps, genomic registration, and mandatory linking of mobile phones to foreign nationals.

The latest trends are reflected in the "Concept of State Migration Policy of the Russian Federation for 2026–2030." This document is even more repressive and concentrated on surveillance and control. Compared to the 2019–2025 version, it places even greater emphasis on the development, implementation, and application of digital technologies for the "monitoring" (i.e., surveillance) of migrants, including a detailed list of such technologies. Thus, amid general statements, the text of this concept explicitly outlines the authorities' intention to further develop and expand: (1) profiling

---

Control, and Increasing Isolation of Internet Users in Russia, Human Rights Watch, July, 2025, https://www.hrw.org/sites/default/files/media_2025/07/russia0725%20web.pdf [accessed November 26, 2025].

[21] United Nations Human Rights Committee, "Concluding Observations on the Eighth Periodic Report of the Russian Federation." *United Nations Human Rights Committee*, 2022, https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=vzwD354mdCl52wdVW7BsB9KX4KJxgSe%2BTbtWWzwb2WhGmoDVuyOe3xxHoXucsUkZU%2Bn5tswtNfD%2FljU7kOdHLA%3D%3D [accessed October 13, 2025].

[22] Since 2014, Crimea, and since the fourth quarter of 2022, the Zaporizhia, Kherson, Donbas, and Luhansk regions of Ukraine have been considered by Russian authorities to be part of the Russian Federation. The UN General Assembly has repeatedly condemned the Russian state's aggressive actions against Ukraine by overwhelming majority votes and does not recognize these territories as part of the Russian Federation. However, Russian authorities have cynically ignored the resolutions. To avoid repetition, it should be clarified that in the text below, the terms "Russia" or "Russian Federation," particularly when referring to events after March 2014, are used not to denote Russian territory within its generally recognized and legal borders, but rather as synonyms for the territory controlled by Russian authorities.

[23] HRW, "Living in Fear and Humiliation. Rising Xenophobic Harassment and Violence towards Central Asian Migrants in Russia." *Human Rights Watch*, March, 2025, https://www.hrw.org/sites/default/files/media_2025/04/russia0325web.pdf [accessed November 23, 2025].

[24] Decree of the President of the Russian Federation No. 622, dated October 31, 2018 "О Концепции государственной миграционной политики Российской Федерации на 2019-2025 годы" (On the Concept of the State Migration Policy of the Russian Federation for 2019–2025), https://www.consultant.ru/document/cons_doc_LAW_310139/74e338ae02b148ec31de4bc38f486b8b045d3a1e/ [accessed November 23, 2025].

data on foreign citizens; (2) the collection of biometric data; (3) notification procedures regarding planned entry; and (4) artificial intelligence–based technologies for "big data processing."[25]

The policy report provides a brief overview of the migrant surveillance system in Russia, or more precisely, in the territory controlled by Russian authorities. The focus is on how this system operates for foreign citizens who decide to travel to Russia, without delving into the intricate structure of the broader Russian surveillance apparatus. A detailed examination would require a far more extensive study and would inevitably involve speculation and conjecture, given that the Russian system is characterized by secrecy, lack of accountability, and complexity. Consequently, this article addresses only some of the known technologies, methods, and strategies employed by Russian authorities to monitor foreign citizens, with an emphasis on developments over the past two years (2024 and 2025). Additionally, it highlights recent regulatory changes that have further expanded the already excessively broad powers of government agencies.

For the purposes of this article, two broad categories of surveillance strategies should be distinguished. The first category focuses primarily on general surveillance, that is, it is aimed either at everyone who falls within the reach of surveillance systems or at large groups of citizens (for example, children, men, women, Black people, street cleaners, migrants). The second category, which can be termed "targeted surveillance," involves tracking the personal data and activities of specific individuals or small groups.[26] Many technologies and methods used for general surveillance—such as video surveillance systems, internet monitoring, migration registration, and tracking financial transactions—can also be employed for targeted surveillance. However, targeted surveillance additionally employs specific techniques and technologies, including external physical surveillance, hacking accounts, using "bugs" and hidden cameras, discreetly installing surveillance software, etc. This article will primarily focus on general surveillance, with an emphasis on the surveillance of migrants. I do not address the targeted surveillance of foreign citizens by Russian authorities in the context of espionage, counterintelligence, or investigative activities, as this is a separate topic shrouded in a particularly thick veil of secrecy.

One final introductory note: for the sake of clarity and convenience, I will present the material in stages. I begin by describing how Russian authorities collect data when a foreign citizen submits an application for a Russian visa or requests entry permission. Next, I discuss the technologies and surveillance methods activated at the moment a foreign citizen enters Russia. Finally, I conclude the narrative with the moment of the migrant's voluntary departure or forced expulsion.

[25] See Decree of the President of the Russian Federation No. 738, dated October 15, 2025 "О Концепции государственной миграционной политики Российской Федерации на 2026-2030 годы" (On the Concept of the State Migration Policy of the Russian Federation for 2026–2030), https://www.garant.ru/hotlaw/federal/1887540/ [accessed November 23, 2025].

[26] In distinguishing between general and targeted surveillance, we rely on Stephen Feldstein's classification of surveillance strategies. However, it is important to note that Feldstein identified four distinct strategies: passive surveillance, targeted surveillance, AI and big-data surveillance, and surveillance laws and directives, see Feldstein, *The Rise of Digital Repression. How Technology Is Reshaping Power, Politics, and Resistance*: 27–30.

1. Submission for Visa and Entry Application: Collection of Personal Information and Biometric Data

The volume of data collected is directly related to the effectiveness of surveillance; therefore, Russian authorities are expanding both the types and the amount of data gathered and are implementing an entry application system for citizens of visa-free countries.

Visas

Visa requirements for visiting Russia vary depending on the purpose of the trip and whether the applicant's country is included in the list of countries eligible for whose citizens it is possible to issue so-called "electronic visas" or not. For those applying for a visa through the usual process, *the Russian Ministry of Foreign Affairs* (hereinafter referred to as *the Russian MFA*)[27] has established an online visa application form available on their official website. This system allows Russian authorities to pre-screen prospective travelers before they submit their documents to the visa department. Subsequently, consular officers require the printed and signed application form, accompanied by a photograph and supporting documents, which vary depending on the applicant and the purpose of the trip. The application form typically requests personal information (full name, date and place of birth, marital status, presence of children, etc.), contact details (phone number, email address, residential address, etc.), and additional information (place of employment, previous visits to Russia, purpose of the trip, accommodation arrangements in Russia, presence of relatives in Russia, etc.).

All this data is entered into the databases of *the Russian MFA*, including *the Automated System for Issuing Invitations to Foreign Citizens* and the *Automated Information System Consul-ZU*,[28] and is then sent to the *Federal Security Service of the Russian Federation* (hereinafter referred to as the *FSB*), which determines whether the citizen is permitted to enter Russia or not. The information is also uploaded to the *State System of Migration and Registration Accounting* (hereinafter referred to as *the MIR*), which is accessible to several other Russian agencies.[29] According to the Decree of the Government of the Russian Federation dated November 7, 2024, the photograph and information obtained during the visa application process are sent to *the Unified Identification and Authentication System*, as well as to the related *Unified Biometric System*.[30]

---

[27] Here and below in the main text, some key government agencies, platforms, programs, legislative acts, organizations, databases, and services involved in the Russian state surveillance system are indicated in italics.

[28] See Order of the Ministry of Foreign Affairs of the Russian Federation No. 9175 dated May 31, 2017, "Об утверждении Порядка организации деятельности Министерства иностранных дел Российской Федерации по оформлению, выдаче, продлению срока действия визы, восстановлению либо аннулированию визы, а также порядка учета и хранения бланков виз" (On the Approval of the Procedure for Organizing the Activities of the Ministry of Foreign Affairs of the Russian Federation Regarding the Registration, Issuance, Extension of Validity, Restoration, or Cancellation of Visas, as well as the Procedure for Recording and Storing Visa Forms), https://base.garant.ru/71709404/ [accessed November 23, 2025].

[29] See paragraph 15 in the Resolution of the Government of the Russian Federation No. 813 dated August 6, 2015 (as amended on October 21, 2024), "Об утверждении Положения о государственной системе миграционного и регистрационного учета, а также изготовления, оформления и контроля обращения документов, удостоверяющих личность" (On Approval of the Regulation on the State System of Migration and Registration Records, as well as the Production, Processing, and Control of the Circulation of Identity Documents), https://www.consultant.ru/document/cons_doc_LAW_184040/ [accessed November 24, 2025].

[30] See paragraph 10 in the Resolution of the Government of the Russian Federation No. 1510 dated November 7, 2024, "О проведении эксперимента по апробации правил и условий въезда в Российскую Федерацию и выезда из Российской Федерации иностранных граждан и лиц без гражданства" (On Conducting an Experiment to Test the Rules and Conditions for Entry into the Russian Federation and Exit from the Russian Federation by Foreign Citizens and Stateless Persons), https://www.garant.ru/products/ipo/prime/doc/410628090/ [accessed November 24, 2025].

In 2021, *the Russian MFA* began issuing so-called "*electronic visas*" to citizens of certain countries. The process for obtaining this type of visa does not require a personal visit to the consulate or visa center and typically takes only a few days. However, unlike regular visas, electronic visas are valid for a single entry and exit and are only applicable for trips lasting no more than 30 days. Additionally, Russian authorities reserve the right to cancel an electronic visa at any time, including during border control, without providing an explanation.[31]

The amount of information required from a foreign citizen seeking to obtain an "electronic visa" is extensive. In addition to standard data—such as full name, sex, marital status, date of birth, purpose of travel, estimated period of stay, and intended address of residence—applicants must provide detailed information, including:

> A list of all countries visited by the applicant in the past three years;
> Personal data of parents, children, and spouse, including their contact information if they reside in Russia;
> Details of any real estate owned in Russia;
> A list of all educational institutions attended by the applicant (excluding schools);
> If applicable, current employment information (and, if this is not the first job, details of the two most recent places of employment);
> A list of instant messaging platforms and social networks used by the applicant;
> Knowledge and education related to "weapons, explosives, nuclear, biological, or chemical substances";
> Level of military training and any participation in military conflicts;
> Information regarding any connection, or lack thereof, with international, non-profit, and government organizations.[32]

All this data and the photograph are uploaded to *the MIR* and other databases, where they are immediately accessed by *the Russian Ministry of Internal Affairs* (hereinafter referred to as *the Russian MIA*) and *the FSB*. These agencies then decide whether to permit or deny entry to the foreign citizen.[33]

Entry Applications

Until 2025, foreign citizens from visa-free countries were not required to prepare special documents for entry into Russia. However, starting in 2025, Russian authorities have implemented an

---

[31] See paragraphs 13 and 14 in the Resolution of the Government of the Russian Federation No. 1793 dated 7 November 2020 "О порядке оформления единых электронных виз и признании утратившими силу некоторых актов Правительства Российской Федерации" (On the Procedure for Issuing Uniform Electronic Visas and the Recognition of Certain Acts of the Government of the Russian Federation as Invalid), https://www.consultant.ru/document/cons_doc_LAW_367444/47e1f3ca06b495c2673ba8e2e466a0feaa84c4f8/ [accessed November 24, 2025].

[32] See Order of the Ministry of Foreign Affairs of Russia No. 22683 dated December 14, 2020 "Об утверждении состава сведений, которые указываются иностранным гражданином в заявлении об оформлении единой электронной визы, а также форм уведомлений об оформлении и об отказе в оформлении единой электронной визы" (On Approval of the Composition of Information to Be Provided by a Foreign Citizen in an Application for a Unified Electronic Visa, as well as Forms of Notifications of Issuance and Refusal to Issue a Unified Electronic Visa), https://base.garant.ru/400103460/ [accessed November 24, 2025].

[33] See paragraphs 15–18 in the Resolution of the Government of the Russian Federation No. 813 dated August 6, 2015 (as amended on October 21, 2024), "Об утверждении Положения о государственной системе миграционного и регистрационного учета, а также изготовления, оформления и контроля обращения документов, удостоверяющих личность" (On Approval of the Regulation on the State System of Migration and Registration Records, as well as the Production, Processing, and Control of the Circulation of Identity Documents), https://www.consultant.ru/document/cons_doc_LAW_184040/ [accessed November 24, 2025].

"experiment," during which foreign citizens arriving from these countries are asked to voluntarily submit an entry application. To do it, the following steps are necessary:

Complete the identification and authentication process on *the Federal State Information System "Unified Portal of State and Municipal Services"* (hereinafter referred to as *Gosuslugi*);
Provide biometric data;
Fill out an entry application form with the required information.[34]

The information listed in the application is compiled and verified by several departments, including *the Russian MFA, the FSB, the Russian MIA*, and *the Russian Ministry of Digital Development, Communications, and Mass Media* (hereinafter referred to as *Minkomsvyaz*). Based on the verification results, the foreign citizen may be notified of a refusal of entry. To facilitate these procedures, the Russian authorities have developed a mobile application for *the Unified Portal ruID* (hereinafter referred to as *ruID*), which was implemented by June 30, 2025. In addition to biometric data (photograph, fingerprints, voice sample) of a foreign citizen wishing to visit Russia without a visa, the application requests personal data (full name, date of birth, citizenship), passport details, purpose of entry, length of stay in Russia, residential address, and contact information. If entry is approved, the foreign citizen receives a QR code, which must be presented for scanning at the border checkpoint.

Based on the information submitted through this app, a "digital profile"—a type of "personal file"—is created for foreign citizens before they cross Russian checkpoints. This file is linked to several information systems, including *Gosuslugi*.[35] Russian authorities do not impose clear restrictions on which agencies can access these digital profiles, the purposes for which it can be used, or the types of information that can be uploaded. Currently, it is known that personal data, biometric data, contact information, document details (passport, migration card, work permit, etc.), border crossing history, place of residence and registration status, medical examination status, tax information, employment history, and social benefits are uploaded to *the "Digital Profile of a Foreign Citizen.*"

Apparently, Russian authorities planned to make the entry application mandatory as early as June 30, 2025. Even the regulatory document itself refers to the "mandatory nature of the experiment."[36] This policy would make entry more difficult for citizens of visa-free countries than for those from visa-required countries, which is in line with the trend pursued by Russian authorities to increase surveillance of labor migrants from Central Asia. However, two weeks before the designated date, *Minkomsvyaz* issued an explanatory letter stating that the absence of an entry application does not currently result in denial of entry.[37] Based on news about *ruID*, the fact that this app was released at

[34] See paragraph 5 in the Resolution of the Government of the Russian Federation No. 1510 dated November 7, 2024, "О проведении эксперимента по апробации правил и условий въезда в Российскую Федерацию и выезда из Российской Федерации иностранных граждан и лиц без гражданства" (On Conducting an Experiment to Test the Rules and Conditions for Entry into the Russian Federation and Exit from the Russian Federation by Foreign Citizens and Stateless Persons), https://www.garant.ru/products/ipo/prime/doc/410628090/ [accessed November 24, 2025].

[35] See Decree of the President of the Russian Federation No. 467, dated July 9, 2025 "О государственном информационном ресурсе 'Цифровой профиль иностранного гражданина'" (On the State Information Resource "Digital Profile of a Foreign Citizen"), https://www.garant.ru/products/ipo/prime/doc/412204934/ [accessed November 24, 2025].

[36] See paragraph 2 in the Resolution of the Government of the Russian Federation No. 1510 dated November 7, 2024, "О проведении эксперимента по апробации правил и условий въезда в Российскую Федерацию и выезда из Российской Федерации иностранных граждан и лиц без гражданства" (On Conducting an Experiment to Test the Rules and Conditions for Entry into the Russian Federation and Exit from the Russian Federation by Foreign Citizens and Stateless Persons), https://www.garant.ru/products/ipo/prime/doc/410628090/ [accessed November 24, 2025].

[37] See Letter of the Ministry of Digital Development of the Russian Federation No. OK-P24-58177 dated June 17, 2025 "О разъяснении правил, вводимых на территории Российской Федерации постановлением Правительства РФ от 07.11.2024 N 1510" (On Clarification of the Rules Introduced in the Territory of the Russian Federation by the

the last minute, and the clarification issued by *Minkomsvyaz*—which does not conduct border control—it can be assumed that Russian authorities have suspended the mandatory application requirement due to serious technical flaws in the system. There is no reason to believe that Russian authorities have altered their plans to make application and registration in *the ruID app* mandatory in the near future.

2. At the Border Crossing Point: Inspection and Additional Data Collection

The Border Service is a division of *the FSB*. At Russian border checkpoints, *FSB* officers verify the authenticity of identity documents and assess whether they have grounds to deny entry. Regardless of whether a foreign citizen has previously submitted biometric data—either when applying for a visa or independently via *ruID—FSB* officers re-collect and verify this data. Refusal to provide biometric data again will result in an entry ban.[38] Additionally, upon entry, foreign citizens complete a migration card, and the information provided is cross-checked by *FSB* officers against the data submitted during the visa or entry application.

The results of all these checks, along with records of border crossings, are immediately entered into *the FSB database*, *the MIR*,[39] the *Unified Identification and Authentication System*,[40] and other databases. Many of these databases are interconnected, and depending on their authority and specific functions, certain government agency employees have access to them. Furthermore, the Russian authorities have developed *the Unified System of Interdepartmental Electronic Interaction*, which enables various government agencies, as well as commercial organizations (primarily banks and financial companies), to exchange information promptly.[41] Cooperation between Russian and Belarusian law enforcement agencies, particularly regarding migration control, has significantly intensified in recent years. As a result, *the MIR* is also supplemented with data from *the Belarusian Border Service* as part of an "information exchange."[42]

Although Russian authorities promise to inform foreign citizens about entry denials, including the reasons for such denials, through their personal accounts, these notifications are for informational purposes only and do not cover all possible grounds.[43] Therefore, even if documents are correctly

---

Resolution of the Government of the Russian Federation No. 1510 dated November 7, 2024), https://www.consultant.ru/document/cons_doc_LAW_509343/ [accessed November 24, 2025].

[38] See article 11 of the Law of the Russian Federation No. 4730-1, dated April 1, 1993, "О Государственной границе Российской Федерации" (On the State Border of the Russian Federation), https://www.consultant.ru/document/cons_doc_LAW_3140/ [accessed November 25, 2025].

[39] See paragraph 12 in the Resolution of the Government of the Russian Federation No. 1510 dated November 7, 2024, "О проведении эксперимента по апробации правил и условий въезда в Российскую Федерацию и выезда из Российской Федерации иностранных граждан и лиц без гражданства" (On Conducting an Experiment to Test the Rules and Conditions for Entry into the Russian Federation and Exit from the Russian Federation by Foreign Citizens and Stateless Persons), https://www.garant.ru/products/ipo/prime/doc/410628090/ [accessed November 24, 2025].

[40] See paragraph 13 Ibid.

[41] See Resolution of the Government of the Russian Federation No. 697, dated September 8, 2010 "О единой системе межведомственного электронного взаимодействия" (On the Unified System of Interdepartmental Electronic Interaction), https://base.garant.ru/199319/ [accessed November 25, 2025].

[42] See subparagraph "b" of paragraph 10, as well as paragraph 35 the Resolution of the Government of the Russian Federation No. 813 dated August 6, 2015 "Об утверждении Положения о государственной системе миграционного и регистрационного учета, а также изготовления, оформления и контроля обращения документов, удостоверяющих личность" (On Approval of the Regulation on the State System of Migration and Registration Records, as well as the Production, Processing, and Control of the Circulation of Identity Documents), https://www.consultant.ru/document/cons_doc_LAW_184040/ [accessed November 24, 2025].

[43] See paragraphs 8 and 9 in the Resolution of the Government of the Russian Federation No. 1510 dated November 7, 2024, "О проведении эксперимента по апробации правил и условий въезда в Российскую Федерацию и выезда из Российской Федерации иностранных граждан и лиц без гражданства" (On Conducting an Experiment to Test the Rules and Conditions for Entry into the Russian Federation and Exit from the Russian Federation by Foreign

completed, an entry application has been submitted, the app has been installed, biometric data has been provided, and no information about a denial is available, Russian authorities may still deny entry to a foreign citizen without providing reasons or explanations.

3. Movement Within Russia: Video Surveillance System

The biometric data collected and verified by *the Russian MFA* and *FSB Border Service* officers at Russian checkpoints serve as the foundation for expanding and enhancing facial recognition systems. These systems utilize advanced technologies, including artificial intelligence, and are integrated with video surveillance networks, enabling the identification and tracking of foreign citizens after they cross Russian border checkpoints.

The active development of Russia's video surveillance system began in Moscow in the 2010s, immediately after Sergei Sobyanin became mayor. *The Unified Data Storage Center* has become the central hub in Moscow for collecting and analyzing video camera data. Moscow authorities have continuously expanded and improved the system, investing substantial resources in it.[44] For example, according to Moscow officials, they planned to spend 26.5 billion rubles, or about 400 million dollars, on the video surveillance system between 2021 and 2023.[45] Video surveillance technology has gradually expanded to other Russian regions. In 2014, the Russian government approved *the Concept for the Construction and Development of the "Safe City" Hardware and Software Complex*.[46] Video surveillance systems—primarily in Moscow—were widely deployed during the 2018 FIFA World Cup and the COVID-19 restrictions of 2020.[47] Following what Russian authorities considered a successful experience, they decided not only to more actively promote surveillance systems in other regions but also to create a unified central data storage and processing system, as revealed by leaks of classified information.[48]

Citizens and Stateless Persons), https://www.garant.ru/products/ipo/prime/doc/410628090/ [accessed November 24, 2025].

[44] Leonid Kovacic, "Сделано не в Китае: как устроена система видеонаблюдения Москвы" [Not Made in China: How Moscow's Video Surveillance System Operates]. *Carnegie Moscow Center*, August 15, 2020, https://carnegie.ru/2020/08/05/ru-pub-82419 [accessed September 19, 2025]; Andrey Zakharov, "'Умный город' или 'Старший брат'? Как мэрия научилась знать о москвичах всё" ["Smart City" or "Big Brother"? How City Hall Has Learned to Know Everything About Muscovites]. *BBC News Russian*, April 10, 2020, https://www.bbc.com/russian/features-52219260 [accessed September 19, 2025]; Evgeny Legalov, "Небольшой брат. Как видеокамеры стали инструментом репрессий" [A Little Brother: How Video Cameras Became a Tool of Repression]. *Radio Svoboda*, May 7, 2024, https://www.svoboda.org/a/neboljshoy-brat-kak-videokamery-stali-instrumentom-repressiy/32932369.html [accessed September 8, 2025].

[45] Roskomsvoboda. "На столичную систему видеонаблюдения потратят порядка 28,5 млрд рублей" [28.5 Billion Rubles Will Be the Capital's Video Surveillance System]. November 10, 2020, https://roskomsvoboda.org/ru/66160/ [accessed September 22, 2025]

[46] See Order of the Government of the Russian Federation No. 2446-r dated December 3, 2014, "Об утверждении Концепции построения и развития аппаратно-программного комплекса 'Безопасный город'" (On Approval of the Concept for the Construction and Development of the Hardware and Software Complex "Safe City"), https://www.consultant.ru/document/cons_doc_LAW_172077/ [accessed November 25, 2025].

[47] Andrey Zakharov, "'Умный город' или 'Старший брат'? Как мэрия научилась знать о москвичах всё" ["Smart City" or "Big Brother"? How City Hall Has Learned to Know Everything About Muscovites]. *BBC News Russian*, April 10, 2020, https://www.bbc.com/russian/features-52219260 [accessed September 19, 2025]; Alexander Borodikhin, "Как устроено 'санитарное дело'" [Corona of Evidence: How the "Sanitary Case" Is Organized]. *Mediazona*, July 7, 2021, https://zona.media/article/2021/07/07/korona-236 [accessed August 5, 2025].

[48] Denis Dmitriev and Liliya Yapparova, "Власти задумали сделать единую систему видеонаблюдения" [The authorities have decided to establish a unified video surveillance system]. *Meduza*, February 29, 2024, https://meduza.io/feature/2024/02/29/vlasti-zadumali-sdelat-edinuyu-sistemu-videonablyudeniya-kak-v-moskve-tolko-po-vsey-strane-iz-utechki-dokumentov-administratsii-prezidenta-my-uznali-kto-ee-razrabatyvaet [accessed September 15, 2025].

Estimates of the number of video cameras used by Russian authorities for surveillance and control vary widely. According to TelecomDaily experts, 18.6 million video surveillance cameras were already in operation in Russia by the end of 2021, 4.8 million of which were equipped with facial recognition capabilities.[49] However, this figure includes all video surveillance cameras, encompassing commercial and private devices. Precise data on the number of cameras used directly by Russian authorities is unavailable. For instance, in 2024, Maksut Shadayev, head of *the Ministry of Digital Development*, stated that there were one million cameras, one-third of which were connected to facial recognition systems.[50] A significant portion of these cameras is located in Moscow, where, according to *the Moscow Government*, 225,000 video surveillance cameras had been installed by mid-2023, nearly all integrated with facial recognition technology. Since there is no independent audit of the number of video surveillance cameras and the methodology behind official figures is unclear, the actual number remains uncertain. For example, data from official regional government portals indicate that in 2023, over half a million cameras were connected to facial recognition systems—significantly more than the number cited by Shadayev.[51] Furthermore, it is unclear whether the figures provided by *the Ministry of Digital Development* refer to cameras installed and maintained by Russian authorities or the total number of cameras accessible to them. If the former, the actual number of cameras accessed by Russian authorities is likely much higher.

Amid the sharp deterioration of the political, economic, and social situation in the Russian Federation, authorities are intensifying efforts to centralize video surveillance systems. For instance, *the Ministry of Digital Development* plans to create and implement a unified federal video surveillance system in 2025–2026, which will consolidate video streams collected from *regional "Safe City" projects*.[52] Video surveillance cameras are being actively installed at border crossings, government buildings, highways, streets, courtyards, entrances, parks, train stations, airports, educational institutions, and public transportation. Authorities are also seeking to leverage the extensive inventory of cameras operated by commercial organizations. According to recent regulatory changes, owners of banks, hotels, stores, shopping centers, cafes, restaurants, and nightclubs are required to install new cameras and connect existing ones to systems accessible by government agencies.[53]

In addition to increasing the number of cameras, linking them to multiple databases, and centralizing data collection and analysis, authorities are enhancing video surveillance systems with

---

[49] TelecomDaily, "В 2022 число камер для ВН в РФ превысит 21 млн" [By 2022, the Number of Video Surveillance Cameras in Russia Will Exceed 21 Million Units]. *TelecomDaily*, September 30, 2022.

[50] Roskomsvoboda, "Каждая третья камера видеонаблюдения подключена к системам распознавания" [Every Third CCTV Camera Is Connected to Facial Recognition Systems]. *Roskomsvoboda*, March 12, 2024, https://roskomsvoboda.org/en/post/kamery-bezgorod-ai/ [accessed September 22, 2025].

[51] Moscow Times, "Три четверти российских регионов внедрили системы слежки за гражданами" [Three-quarters of Russian Regions Have Implemented Citizen Surveillance Systems]. *Moscow Times*, October 24, 2023, https://www.moscowtimes.ru/2023/10/24/tri-chetverti-rossiiskih-regionov-vnedrili-sistemi-slezhki-za-grazhdanami-a111011 [accessed September 22, 2025]

[52] Anastasia Gavrylyuk, "Сдутая камера: Минцифры намерено создать платформу видеонаблюдения за 2 млрд рублей" [Deflated Camera: The Ministry of Digital Development, Communications and Mass Media Wants Create a Video Surveillance Platform for 2 Billion Rubles]. *Forbes Russia,* January 13, 2025.

[53] Roskomsvoboda, "В Москве хотят подключить камеры ТЦ к городской системе видеонаблюдения" [The Moscow Goverment Plans to Integrate Shopping Center Cameras into the City's Video Surveillance System]. *Roskomsvoboda*, October 20, 2021, https://roskomsvoboda.org/en/post/kamery-maski-kontrol/ [accessed September 24, 2025]; Moscow Times, "'Отказаться нельзя'. Гостиницы Москвы обязали подключиться с государственной системе видеослежки за гражданами" ["No Refusal." Moscow Hotels Required to Join State Citizen Video Surveillance System]. *Moscow Times,* October 19, 2022, https://www.moscowtimes.ru/2022/10/19/otkazatsya-nelzya-gostintsi-moskvi-obyazali-podklyuchitsya-s-gosudarstvennoi-sisteme-videoslezhki-za-grazhdanami-a25487 [accessed September 25, 2025]; Roskomsvoboda, "Столичная мэрия заглянет в ночные клубы... через камеры видеонаблюдения" [The Capital City's Mayor's Office Will Peek into Nightclubs... through CCTV Cameras]. *Roskomsvoboda*, May 4, 2022, https://roskomsvoboda.org/en/post/podglyadet-za-nochikami/ [accessed September 24, 2025].

new technologies that incorporate increasingly sophisticated facial recognition algorithms. These algorithms can identify individuals even under poor surveillance conditions or when their faces are significantly obscured by clothing or medical masks.[54] Furthermore, programs that recognize people by their silhouettes and gait are being implemented. Authorities are also deploying technologies capable of detecting emotions, ethnicity, and determining whether a person is considered a "friend" or "foe" within a given environment. Numerous information systems and software solutions exist, varying according to their intended use, agency, region, and specific technology.

The introduction of video surveillance systems was accompanied by declarations that these technologies were necessary to more effectively combat crime and ensure public safety. However, from the outset, these systems were also designed to suppress political opposition, as evidenced even in regulatory documents. For example, *the federal "Safe City" concept* lists several action which it defines as "threats," including:

> Any public event or action unauthorized by Russian authorities;
> Informational influence on the population through the media and the Internet that Russian authorities consider "negative";
> "Incomplete realization of citizens' rights to receive and exchange reliable information, including manipulation of mass consciousness through informational and psychological influence";
> Information from "media outlets," including content published on the Internet, which Russian authorities mark as provoking "social, interethnic, and religious tensions."[55]

These vague and broad formulations initially allowed for abuse, such as classifying any street protest or online criticism of the authorities as "threats." Indeed, Russian authorities have actively used video surveillance systems to suppress opposition, persecute journalists and civil society activists, and advance other repressive political objectives.[56]

Although the video surveillance system is designed to monitor and control both Russian and foreign citizens, some regions are implementing innovations aimed primarily at migrants. For example, in 2025, *the Moscow government* mandated that all construction sites be equipped with video surveillance systems connected to *the Unified Data Storage Center*.[57] St. Petersburg explicitly announced the implementation of a system for recognizing individuals' "ethnicity" under

---

[54] Anastasia Gavrylyuk, "Контрольная работа: городские камеры научат слышать звуки и распознавать силуэты" [Test: City Cameras Will Understand Sounds and Recognize Silhouettes]. *Forbes Russia*, February, 13, 2024.

[55] See Order of the Government of the Russian Federation No. 2446-r dated December 3, 2014, "Об утверждении Концепции построения и развития аппаратно-программного комплекса 'Безопасный город'" (On Approval of the Concept for the Construction and Development of the Hardware and Software Complex "Safe City"), https://www.consultant.ru/document/cons_doc_LAW_172077/ [accessed November 25, 2025].

[56] Andrei Soldatov and Irina Borogan, *Digital Surveillance and the Impact on Journalism in Russia*. Friedrich Naumann Foundation for Freedom, 2020, https://shop.freiheit.org/#!/Publikation/943 [accessed August 18, 2025]; OVD-Info, "Как власти используют камеры и распознавание лиц против протестующих" [How Russian Authorities Are Using Cameras and Facial Recognition Against Protesters]. *OVD-Info*, February 17, 2022, https://reports.ovd.info/kak-vlasti-ispolzuyut-kamery-i-raspoznavanie-lic-protiv-protestuyushchih [accessed September 25, 2025]; IPHR and Global Diligence. *Russia's Digital Authoritarianism: the Kremlin's Toolkit.* International Partnership for Human Rights (IPHR) and Global Diligence LLP, 2023, https://iphronline.org/articles/russias-digital-authoritarianism-the-kremlins-toolkit/ [accessed November 22, 2025]; OVD-Info and Roskomsvoboda, "Human Rights and New Technology in Russia". *OVD-Info and Roskomsvoboda,* March 6, 2023, https://ovd.info/en/human-rights-and-new-technology-russia?utm_source=google.com&utm_medium=organic&utm_term=%28not+set%29#1-6 [accessed November 25, 2025].

[57] See Resolution of the Moscow Government No. 47-PP dated January 21, 2025 "О внесении изменений в постановления Правительства Москвы от 16 июня 2011 г. N 272-ПП и от 19 мая 2015 г. N 299-ПП" (On Amendments to the Moscow Government Resolutions dated June 16, 2011, No. 272-PP, and May 19, 2015, No. 299-PP), https://www.consultant.ru/law/review/209259861.html [accessed November 25, 2025].

surveillance, openly acknowledging that this system will be used to monitor and control migrants.[58] It is likely that other regions, as well as federal authorities, are implementing additional projects based on video surveillance systems aimed specifically or primarily at monitoring foreign citizens.

For several years, it has been known that Russian authorities use facial recognition systems, among other methods, to detain foreign citizens they consider to be "illegally" present in Russia. In 2020, *the Russian MIA* announced the implementation of artificial intelligence technologies to identify such migrants. A recent major operation in Moscow exemplifies this practice: with the apparent assistance of *the State Automated Information System "Sfera"* (Сфера)[59] employed by police officers in *the Moscow metro*, a mass detention of foreign nationals suspected of violating immigration regulations was conducted.[60] Notably, Russian law enforcement agencies have previously utilized *"Sfera"* for the preventive detention of journalists, civil society activists, and opposition figures.[61]

Tracking physical movements through video surveillance systems is closely intertwined with online surveillance. For example, high-quality photographs submitted by foreign citizens for visa or entry applications allow Russian authorities not only to locate these individuals on streets, public transportation, and in buildings but also to identify them on social media and in images and videos posted online. This process also works in reverse: individuals depicted in photographs or videos posted online can be detected by video surveillance systems. Therefore, although it may be convenient to distinguish between video surveillance and online surveillance, the boundaries between the two are often blurred.

4. Internet Use: Monitoring and Censorship

Upon crossing Russian border checkpoints, foreign citizens are first denied or restricted access to numerous social platforms (e.g., LinkedIn, Instagram, Facebook, X), messaging apps (e.g., WhatsApp, Signal, Discord, Viber, Telegram), services (e.g., Patreon, Amazon, Google Play), and global news sites (e.g., BBC, Deutsche Welle, Radio Liberty). Second, Russian authorities begin monitoring their online activities. Third, foreign citizens face the risk of administrative or criminal liability for various online actions.[62] For example, recently, Russian authorities expanded the list of prohibited online activities that may result in administrative penalties to include merely searching for and viewing materials that the authorities regard as extremist, and the use of a VPN may be considered an aggravating factor.[63]

---

[58] Roskomsvoboda, "Петербургские видеокамеры научили распознавать этническую принадлежность" [St. Petersburg Video Cameras Have Been Programmed to Recognize Ethnicity]. *Roskomsvoboda,* August 25, 2025, https://roskomsvoboda.org/ru/post/ethnicity-detection-cctv-russia-policy/ [accessed September 26, 2025].

[59] See Resolution of the Moscow Government No. 328-PP dated March 17, 2021 "О государственной автоматизированной информационной системе 'Сфера'" (On the State Automated Information System "Sfera"), https://base.garant.ru/400484831/ [accessed November 25, 2025].

[60] Memorial HRDC, "Mass detentions of migrants across Russia". *Memorial Human Rights Defence Centre*, Juny 20, 2024, https://memorialcenter.org/en/news/mass-detentions-of-migrants-across-russia [accessed September 26, 2025].

[61] Paper, "Как оппозиционеров задерживают с помощью распознавания лиц. Рассказываем о московской системе 'Сфера' и ее аналоге в Петербурге" [How Opposition Activists Are Detained by Facial Recognition Technology. We Examine Moscow's "Sfera" System and Its Counterpart in St. Petersburg]. *Paper*, Juny 15, 2022, https://paperpaper.io/kak-oppozicionerov-zaderzhivayut-s-pom/ [accessed September 26, 2025].

[62] HRW, "Disrupted, Throttled, and Blocked State Censorship, Control, and Increasing Isolation of Internet Users in Russia," *Human Rights Watch*, July, 2025, https://www.hrw.org/sites/default/files/media_2025/07/russia0725%20web.pdf [accessed November 26, 2025].

[63] Sergei Dick and Olga Tikhomirova, "Наказание за поиск в Сети. Какие штрафы грозят россиянам" [Punishments for Internet Searches: What Fines Russians Face]. *Deutsche Welle,* July 23, 2025, https://www.dw.com/ru/nakazanie-za-poisk-v-internete-kakie-strafy-grozat-rossianam/a-73388354 [accessed September 11, 2025].

Russian authorities primarily conduct surveillance and control of telephone and internet communications through *the System of Operational Investigative Measures* (hereinafter referred to as *SORM*). This system comprises a set of organizational, regulatory, and technological tools that enable the tracking, storage, and analysis of data collected from telephone and internet traffic. *The FSB* implements and oversees *SORM*, which originated during the era of the KGB. In the 1990s, *SORM* was initially designed for wiretapping telephone conversations. Internet surveillance was subsequently incorporated and has since become increasingly sophisticated and pervasive. For many years, *the FSB* has openly monitored internet traffic to and from the territories controlled by Russian authorities particularly through the installation of *SORM* equipment and the physical presence of its officers at major internet exchange points within the country.[64]

Gradually, Russian authorities compelled all telecom operators, providers, and even Russian internet services offering telephone and internet services to implement and participate in *the SORM system*.[65] Russian authorities remained undeterred by the fact that, as early as 2015, the European Court of Human Rights ruled that *the SORM system* was susceptible to abuse and non-compliant with the European Convention on Human Rights (see Zakharov v. Russia). On the contrary, since then, Russian authorities have strengthened and expanded the system's scope. A key measure to enhance the powers of intelligence agencies and improve surveillance was the adoption of the so-called *"Yarovaya Law,"* which primarily shifted the costs associated with user surveillance to companies—for example, requiring them to store all internet traffic for 30 days and connection data for six months (*Federal Laws of July 6, 2016, No. 374-FZ* and *July 6, 2016, No. 375-FZ*). Since then, Russian authorities have enacted several other regulations aimed at similar objectives. Moreover, if a company refuses to cooperate closely with intelligence agencies, the authorities typically identify various "violations" and, if noncompliance persists, revoke its license. As a result, Russian mobile operators, internet providers, internet services, and data storage facilities are closely linked to intelligence agencies, which have 24/7 and virtually unlimited access to user data, transactions, and correspondence.[66]

Recent news indicates that Russian authorities have decided not only to grant law enforcement agencies open and virtually unlimited access to the data of telecom operators, service providers, and website owners but have also taken steps to actively compel these entities to conduct surveillance and report about "signs of wrongdoing." (Korzhova 2025).[67]

Internet surveillance is also conducted within the framework of the so-called "sovereign internet" concept. The primary coordinator for implementing this concept is *Roskomnadzor*, specifically two of its structural units: the *Main Radio Frequency Center* (Главный радиочастотный центр) and the *Public Communications Network Monitoring and Control Center* (Центр мониторинга и

---

[64] Andrei Soldatov and Irina Borogan, *The Red Web. The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries* (PublicAffairs, 2015).

[65] See Resolution of the Government of the Russian Federation No. 743, dated July 31, 2014, "Об утверждении Правил взаимодействия организаторов распространения информации в информационно-телекоммуникационной сети 'Интернет' с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации" (On Approval of the Rules for Interaction Between Organizers of Information Dissemination in the Information and Telecommunications Network "Internet" and Authorized Government Agencies Conducting Operational-Search Activities or Ensuring the Security of the Russian Federation), https://base.garant.ru/70709018/ [accessed November 11, 2025].

[66] Valeria Pozychanyuk and Petro Mironenko, 2"ФСБ потребовала от интернет-сервисов онлайн-доступ к данным и переписке пользователей" [The FSB has demanded that internet service providers grant online access to users' data and correspondence]. *The Bell*. February 11, 2020, https://thebell.io/fsb-potrebovala-ot-internet-servisov-onlajn-dostup-k-dannym-i-perepiske-polzovatelej [accessed October 1, 2025].

[67] Daria Korzhova, "Самозапреты и отключения: власти запланировали меры по защите граждан в интернете" [Self-Prohibitions and Shutdowns: Authorities Plan Measures to Protect Citizens Online]. *Forbes Russia,* August 21, 2025.

управления сетью связи общего пользования).[68] *Roskomnadzor* is responsible for mass website blocking, traffic restrictions, slowing down platforms that refuse to cooperate with Russian systems, and constructing the so-called "Russian segment of the internet," whose main principles are alignment with official propaganda and accountability to *Roskomnadzor* and law enforcement agencies.[69]

Surveillance of social media and messaging apps deserves special mention. It is well known that Russian social media and messaging platforms closely cooperate with Russian authorities and are typically fully transparent to security services. Regarding foreign social media and messaging apps, the authorities employ three main strategies:

1. Suppression or outright bans have been imposed on popular messaging apps and social networks such as WhatsApp, Signal, LinkedIn, Discord, Viber, Telegram, Facebook, Instagram, and X, which have been blocked or partially restricted in Russia;

2. Pressure to achieve full cooperation—for example, the Russian government's well-documented history of pressuring the messaging app and social network Telegram, even despite journalists uncovering some evidence suggesting possible access by Russian intelligence services to Telegram users' correspondence[70];

3. Development and use of technologies and malware that enable unauthorized access to confidential correspondence and data. For example, experts report that Russian intelligence services employ various surveillance programs to hack and bypass the security of well-known foreign messaging apps.[71]

As demonstrated by the recent blocking of WhatsApp video calls, Russian authorities are primarily focused on excluding all Western telecommunications and internet companies, replacing foreign social media and messaging apps with Russian "analogues" that are fully controlled by individuals affiliated with the government and are transparent to law enforcement agencies.

The most popular Russian social network among both Russian citizens and migrant workers is *VKontakte*, with approximately 90 million monthly users. *VKontakte* is owned by *VK Holding*, which also includes *the Odnoklassniki social network* (also popular among migrants), *the email service "Pochta"* (Почта), *the blogging and news platform "Zen"* (Дзен), *the classifieds service "Yula"* (Юла), *the educational platform "Uchi.ru"* (Учи), and other internet services. *VK Holding* is an important component of the surveillance system for internet platforms and messaging apps

---

[68] See Resolution of the Government of the Russian Federation No. 136 dated February 13, 2019 "О Центре мониторинга и управления сетью связи общего пользования" (On the Center for Monitoring and Control of the Public Communications Network), https://base.garant.ru/72180742/ [accessed November 26, 2025] and Order of Roskomnadzor No. 225 dated July 31, 2019 "Об утверждении Положения о Центре мониторинга и управления сетью связи общего пользования" (On the Approval of the Regulation for the Center for Monitoring and Control of the Public Communications Network), https://www.consultant.ru/document/cons_doc_LAW_338375/5ca8c9d8a91fec8a0bb0794025b7f411b9b705f8/ [accessed November 26, 2025].

[69] Alena Epifanova, *Deciphering Russia's "Sovereign Internet Law." Tightening Control and Accelerating the Splinternet,* (German Council on Foreign Relations, 2020), https://dgap.org/sites/default/files/article_pdfs/dgap-analyse_2-2020_epifanova_0.pdf [accessed October 17, 2025]; Andrei Soldatov and Irina Borogan. *The New Iron Curtain. The Center for European Policy Analysis (CEPA)*. June 7, 2022, https://cepa.org/comprehensive-reports/the-new-iron-curtain-2/ [accessed October 13, 2025].

[70] Sergey Kagermazov and Anna Popova, "Не самый надежный мессенджер? Основные вопросы о Telegram" [Not the Most Reliable Messenger? Main Questions About Telegram]. *BBC News Russian*, June 11, 2025, https://www.bbc.com/russian/articles/c0lndgzwwn1o [accessed October 2, 2025].

[71] Krolik, Aaron, Paul Mozur, and Adam Satariano, "Cracking Down on Dissent, Russia Seeds a Surveillance Supply Chain," *The New York Times*, July 3, 2023, https://www.nytimes.com/2023/07/03/technology/russia-ukraine-surveillance-tech.html [accessed August 19, 2025].

being developed by Russian authorities. It is no coincidence that in 2021, the company came under direct state control when *Gazprom* acquired its controlling stake, and Vladimir Kirilenko, the son of the *Kremlin* chief of staff, became CEO.[72] Consequently, *VK's platform services* are extensively used by Russian authorities for surveillance, persecution, manipulation, disinformation, and trolling.[73]

It is unsurprising that Russian authorities selected *VK Holding* to develop a replacement for WhatsApp. Russian companies had long attempted to create a "domestic" messenger but had failed to achieve success, leaving WhatsApp as the most popular app among Russian users. The situation changed in mid-2025 due to direct intervention by government agencies. Consequently, in 2025, *VK Holding* completed the development of *Max messenger*, which was immediately approved by the Russian government as the "national Russian messenger" and began to be actively promoted through state influence. Simultaneously, a vigorous media propaganda campaign against WhatsApp was launched, followed by its gradual blocking to compel users to switch to *Max messenger*.

Max messenger is a powerful new tool within the Russian authorities' surveillance system. For instance, its Privacy Policy explicitly states that it collects data on users' locations, browsers, installed apps, contacts, IP addresses, and all actions performed within the service. Additionally, at its discretion, it shares this data with third parties, including government agencies. This is only what the developers openly acknowledge.[74] The program may also include undisclosed functionalities, such as password retrieval, unauthorized access to the microphone and camera, screenshot capture, and similar capabilities. Notably, unlike WhatsApp, *Max messenger* lacks end-to-end encryption, and its encryption system was developed by *the FSB*.[75] These factors make *Max messenger* comparable to its Chinese counterpart, WeChat, which is known for its complete transparency to Chinese authorities and has long been used as a tool for surveillance, propaganda, control, harassment, and censorship.[76] Russian authorities have not concealed the fact that *Max messenger* is modeled after its Chinese counterpart. They are so invested in implementing this convenient surveillance tool that they have mandated installing *Max app* on all smartphones starting in September 2025.[77]

---

[72] Meduza, "VK перешел под контроль Газпромбанка и 'Согаза' друга Путина Юрия Ковальчука. Гендиректором VK станет сын Сергея Кириенко" [VK Has Come Under the Control of Gazprombank and Sogaz, Both Owned By Yuri Kovalchuk, a Close Associate of Vladimir Putin. Sergei Kiriyenko's Son Is Set to Become VK's CEO]. *Meduza*, December 3, 2021, https://meduza.io/feature/2021/12/03/vk-pereshel-pod-kontrol-gazprombanka-i-sogaza-druga-putina-yuriya-kovalchuka-gendirektorom-vk-stanet-syn-sergeya-kirienko [accessed October 2, 2025].

[73] Philipp Dietrich, *The Key Player in Russia's Cybersphere. What the West Needs to Know about VK Company*. (German Council on Foreign Relations, 2023), https://dgap.org/en/research/publications/key-player-russias-cybersphere [accessed October 2, 2025].

[74] Insider, "VK представила 'российский WeChat': приложение получает доступ к микрофону, камере и передает данные властям. Главное о мессенджере" [VK Has Unveiled a "Russian WeChat": the App Accesses the Microphone And Camera And Shares Data With Authorities. Here Are the Key Facts About the Messenger]. *Insider*, Juny 5, 2025, https://theins.ru/news/281890 [accessed October 13, 2025].

[75] Aleksej Aleksandrov, "В России начали широко рекламировать мессенджер Max. В чем его опасность и способен ли он стать аналогом китайского WeChat?" [In Russia, Messenger Max has been widely advertised. What are its dangers and is it possible for it to become a Chinese WeChat equivalent?]. *Current Time TV*, July 14, 2025, https://www.currenttime.tv/a/v-rossii-nachali-shiroko-reklamirovat-messendzher-max-v-chem-ego-opasnost-i-sposoben-li-on-stat-analogom-kitayskogo-wechat-/33472932.html [accessed September 4, 2025].

[76] Kócsi, Bence, and Benjamin Finn. "Investigating WeChat: An introduction to social apps WeChat and Weixin." *Reporters Without Borders*, August 12, 2024, https://safety.rsf.org/investigating-wechat-an-introduction-to-social-apps-wechat-and-weixin/ [accessed October 3, 2025].

[77] Meduza, "Мессенджер Max начнут предустанавливать на все смартфоны в России с 1 сентября" [Messenger Max Will Be Pre-installed on All Smartphones in Russia Starting September 1]. *Meduza*, August 21, 2025, https://meduza.io/news/2025/08/21/messendzher-max-stanut-predustanavlivat-na-vse-smartfony-v-rossii-s-1-sentyabrya [accessed October 2, 2025].

While the "Russian segment" of the internet is not yet fully isolated from the "global network," it is clear that authorities are actively preparing for such a scenario. This is evidenced not only by the exclusion of the last remaining Western companies and services but also by regular internet shutdowns, a rapidly increasing number of blocked websites, public tests of disconnection from the "global network," and the creation of a so-called "white list of sites," which, according to Russian authorities, must remain accessible during shutdowns.[78]

In addition to the ongoing connection to the World Wide Web, another significant surveillance concern for Russian authorities—particularly regarding mobile internet and telephony—is the widespread use of anonymous SIM cards. That is why Russian officials have introduced new regulations aimed at preventing this form of surveillance circumvention, with some measures specifically aimed at foreign citizens. According to the new law, effective January 1, 2025, foreign citizens can only enter into communication contracts at mobile phone stores, and each SIM card must be linked to a specific mobile device via its IMEI (International Mobile Equipment Identity) number. Furthermore, in addition to providing proof of identity, foreign citizens must also submit their "*SNILS"* (Individual Insurance Account Number), have an account on *Gosuslugi*, and complete registration and biometric verification when signing a contract. *Amendments to the Law "On Communications" in 2024* extend this biometric verification requirement to those who entered into contracts previously.[79] Since July 1, 2025, mobile operators have begun suspending services for foreign citizens who fail to provide biometric confirmation. At the beginning of summer 2025, authorities reported that approximately 2 million foreign citizens had submitted their biometric data to continue using Russian mobile communications.[80]

Russian authorities believed that simply documenting and technically linking a specific telephone number and mobile device to an individual was insufficient; they considered it essential that the person never relinquish possession of the device. This likely explains why Russian authorities enacted *Federal Law No. 41-FZ dated April 1, 2025* that further expanded the powers of law enforcement agencies, including granting them access to banking information. Most importantly, given the focus of our review, the law prohibits the transfer of mobile phones and SIM cards to others, except to relatives or in certain emergency situations.[81]

---

[78] Kirill Shestakov, "В РФ проводят учения по отключению от зарубежного интернета" [Russia Is Conducting Exercises to Disconnect From the Foreign Internet]. *Detusche Welle*, December 6, 2024, https://www.dw.com/ru/v-rossii-provodat-ucenia-po-otkluceniu-ot-zarubeznogo-interneta/a-70989516 [accessed October 7, 2025]; Natalia Glukhova and Lyubov Borisenko, "Going dark. Digital shutdowns are at an all-time high in Russia, with those in power now able to turn off mobile internet at will". *Novaya Gazeta Europe*, July 8, 2025, https://novayagazeta.eu/articles/2025/07/22/going-dark-en [accessed September 11, 2025]; Verstka, "Власти ограничили доступ к рекордному числу сайтов в 2024 году – более чем к 417 тысячам" [Authorities Restricted Access To a Record Number of Websites in 2024—More Than 417,000]. *Verstka*, January 28, 2025, https://verstka.media/vlasti-ogranichili-dostup-k-rekordnomu-chislu-saitov-v-2024-godu-bolee-chem-k-417k-news [accessed August 20, 2025]; Roman Kohantes, "Russian Belgorod, Rostov Switch to "Whitelist" Mobile Internet, Allow Only Kremlin-Approved Sites," *United24 Media*, November 27, 2025, https://united24media.com/latest-news/russian-belgorod-rostov-switch-to-whitelist-mobile-internet-allow-only-kremlin-approved-sites-13807 [accessed December 2, 2025].

[79] See Federal Law No. 303-FZ dated August 8, 2024 "О внесении изменений в Федеральный закон 'О связи' и отдельные законодательные акты Российской Федерации" (On Amendments to the Federal Law "On Communications" and Certain Legislative Acts of the Russian Federation), https://www.consultant.ru/document/cons_doc_LAW_482565/ [accessed November 26, 2025].

[80] Jean Rofe, "Иностранцев в РФ, не сдавших биометрию, лишат сим-карт" [Foreigners, Who Fail to Submit Biometrics, Will Be Deprived of SIM Cards]. *Deutsche Welle*, July 1, 2025, https://www.dw.com/ru/inostrancev-v-rossii-ne-sdavsih-biometriu-lisat-simkart/a-73109351 [accessed September 17, 2025].

[81] See Federal Law No. 41-FZ dated April 1, 2025 "О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации" (On the Creation of a State Information System for Combating Offenses Committed Using Information and Communication

Regarding migration, it is also important to note that Russian authorities are exporting their surveillance systems and equipment to Cuba, Venezuela, Belarus, and Central Asian countries such as Uzbekistan, Kyrgyzstan, and Kazakhstan. As highlighted in a report by the cybersecurity firm Recorded Future, Russian intelligence services likely maintain access to the exported devices.[82]

5. Communication: Voice Recognition

In addition to photographs, Russian authorities have increasingly focused on collecting voice samples from migrants. This development is closely linked to the expanding use of speech recognition technologies in Russia.

Modern technology enables the accurate identification of individuals by their voice, which necessitates storing voice samples in a database for comparison. *The Russian government*'s intent to amass as many voice samples as possible likely explains why banks in Russia were authorized to implement voice identification technologies in 2018. This authorization coincided with the launch of the state-run *Unified Biometric System*, to which banks began submitting their clients' biometric data.[83] Although banks are formally required to obtain consent for such data transfers, it cannot be ruled out that all or most of the collected voice samples were included in *the Unified Biometric System*.[84] Notably, some of the earliest adopters of voice recognition technology were such giants as *Sberbank, VTB, Gazprombank, Rosselkhozbank*, and *Pochta Bank*, all of which are state-owned and closely affiliated with *the Russian government.*

Voice recognition technologies have also been integrated into *Gosuslugi*, multifunctional centers (budgetary organizations that provide state and municipal services), and even *Russian Post services.* Consequently, foreign citizens wishing to use *Gosuslugi* or visit *multifunctional centers (МФЦ)* will likely be asked to provide a voice sample, which will be uploaded to *the Unified Biometric System* and made accessible to numerous government agencies. Furthermore, in December 2022, Russian authorities enacted a law mandating *multifunctional centers*, along with various other state, municipal, and private organizations, to transfer biometric data to *the Unified Biometric System*.[85]

Overall, foreign citizens have increasingly limited options for avoiding the submission of their voice samples to the state system. As noted, on July 1, 2025, Russian telecom operators began requiring verified biometric data, including voice samples, as a condition for initiating or continuing services. The apparent objective is to enable the identification of any foreign citizen residing in Russia not only through video and photography but also by voice. This facilitates intelligence

---

Technologies, and on Amendments to Certain Legislative Acts of the Russian Federation), https://www.consultant.ru/document/cons_doc_LAW_502182/ [accessed November 26, 2025].

[82] Insikt Group. *Tracking Deployment of Russian Surveillance Technologies in Central Asia and Latin America* (Insikt Group, 2025), https://go.recordedfuture.com/hubfs/reports/ta-ru-2025-0107.pdf [accessed August 20, 2025].

[83] See Federal Law No. 482-FZ dated December 31, 2017 "О внесении изменений в отдельные законодательные акты Российской Федерации" (On Amendments to Certain Legislative Acts of the Russian Federation), https://www.garant.ru/products/ipo/prime/doc/71748784/ [accessed]November 27, 2025].

[84] Marina Dulneva, "Тинькофф и Сбербанк теперь передают биометрические данные клиентов властям" [Tinkoff and Sberbank Share Their Clients' Biometric Data with Russian Authorities]. *Meduza*, October 12, 2023, https://meduza.io/cards/tinkoff-i-sberbank-teper-peredayut-biometricheskie-dannye-klientov-vlastyam-chem-opasno-hranenie-takih-dannyh-v-gosudarstvennoy-sisteme-i-kak-zapretit-ih-ispolzovat [accessed October 7, 2025].

[85] See Federal Law No. 572-FZ dated December 28, 2022 "Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации" (On the Implementation of Identification and/or Authentication of Individuals Using Biometric Personal Data, Amendments to Certain Legislative Acts of the Russian Federation, and the Recognition of Certain Provisions of Legislative Acts of the Russian Federation as Invalid), https://www.consultant.ru/document/cons_doc_LAW_436110/ [accessed November 27, 2025].

agencies' ability to eavesdrop on telephone conversations and voice messages, as well as conduct surveillance wherever voice recordings are made (e.g., *multifunctional centers*, offices of many banks and government agencies, telephone consultations, etc.).

Several Russian companies are developing voice recognition technologies, including *MTS, Yandex, Inlexis, DSS Lab, Clarity, Naumen*, and *ASM Solutions*. Notably, the most significant company for the Russian authorities—effectively state-owned—is the *Center for Speech Technologies*. Founded in 1990 based on developments originally controlled by the KGB, the *Center for Speech Technologies* has been owned by *Sberbank* (formerly *Gazprombank*) since 2019. The company offers a range of products, such as AgentNavigator, which creates AI agents with voice recognition capabilities; the "Charlie" program, which handles speech recognition and text conversion; and Voice2Med, a program that converts spoken medical personnel documents into text. Of particular importance is the *VoiceKey platform,* which includes the *VoiceKey.INSPECTOR* biometric data collection program integrated with *the Unified Biometric System*. Among the *Center for Speech Technologies'* clients are numerous central government agencies, including law enforcement bodies.[86]

6. Use of Transport Vehicles and Staying at Hotels: Verification of Movements

Hotels, hostels, resorts, and other hospitality businesses record the arrival and departure of foreign citizens and register this information with migration authorities. Until recently, these businesses transmitted data on foreign guests to *the Russian MIA* using various programs (e.g., *АИС "ЭЛПОСТ," Скала-гостиница, Контур.ФМС*). However, starting in 2024, in an apparent effort to centralize and standardize data flow, Russian authorities have implemented this function through *Gosuslugi*, eliminating the need for intermediary programs. Hospitality businesses are now required to submit notifications of both the arrival and departure of foreign citizens within one business day. The arrival notification must include personal data (full name, date and place of birth, sex, citizenship), place of registration, period of stay, and passport number and series. A copy of the guest's passport and migration card must be attached to the notification. It is evident that, in addition to *the Russian MIA*, many other state agencies have access to data on foreign citizens staying at Russian hospitality establishments.

Furthermore, authorities have implemented hotel registration through *the Unified Identification and Authentication System*, enabling the immediate recording of all guests and the collection of biometric data. In 2022, Moscow authorities went even further by strongly recommending—effectively mandating—that hotels and hostels connect their video surveillance cameras to the state-run system.[87]

For a long time, purchasing a ticket and boarding a long-distance train in Russia has required filling out a form and presenting an identity document, a common practice worldwide. However, a less common—and mandatory—requirement in Russia is the installation of video surveillance systems inside each train car, along with the extensive volume and detail of data collected.[88] Similar to hotel

[86] See Soldatov and Borogan, *The Red Web. The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*.

[87] Moscow Times, "'Отказаться нельзя'. Гостиницы Москвы обязали подключиться с государственной системе видеослежки за гражданами" ["No Refusal." Moscow Hotels Required to Join State Citizen Video Surveillance System]. *Moscow Times*, October 19, 2022, https://www.moscowtimes.ru/2022/10/19/otkazatsya-nelzya-gostintsi-moskvi-obyazali-podklyuchitsya-s-gosudarstvennoi-sisteme-videoslezhki-za-grazhdanami-a25487 [accessed September 25, 2025].

[88] See Resolution of the Government of the Russian Federation No. 969 dated September 26, 2016 "Об утверждении требований к функциональным свойствам технических средств обеспечения транспортной безопасности и Правил обязательной сертификации технических средств обеспечения транспортной безопасности" (On the Approval of Requirements for the Functional Properties of Technical Equipment Ensuring Transport Security and the

registration, biometric identification for purchasing tickets and boarding trains was introduced in 2025. While some users find this convenient, the system also facilitates increased surveillance and the collection of biometric data.[89]

The installation of surveillance video cameras also applies to intercity buses. Information on the movements of Russian and foreign citizens is collected in *the Automated Centralized Database of Personal Data on Passengers and Vehicle Personnel*, which is part of *the Unified State Information System for Transport Security*.[90]

Using public transportation is also becoming increasingly less anonymous. *Metro systems* in major cities are equipped with numerous cameras, including hidden ones. In Moscow, cameras are installed not only in tunnels, platforms, and vestibules but also in every train car. Additionally, cameras are now being mandated on buses and trams. This practice, initially implemented in Moscow, is gradually spreading to other Russian cities.

Russian authorities are also closely monitoring taxi passengers. Taxi bookings are typically made through Russian services and apps that share user data with law enforcement agencies.[91] Some Russian politicians considered this insufficient, and at the end of 2024, a bill was introduced in *the State Duma* to mandate the installation of surveillance cameras in all taxis.[92] Although the bill was not passed, it clearly demonstrates the intention to ensure total surveillance, and many taxis are already equipped with cameras.

Overall, tens of thousands of traffic cameras monitor vehicle movements and are connected to *the State Traffic Safety Inspectorate's Centralized Information and Analytical System "Web"* (Паутина). In addition to standard video recording and license plate recognition, some of these cameras can also identify the faces of drivers and front-seat passengers, and occasionally even rear-seat passengers—although the accuracy of facial recognition for the latter remains questionable. However, the exact number of traffic cameras, estimated to be between 30,000 and 50,000 units as of 2024, and how many are connected to the facial recognition system remain unknown.

7. Registration by Migration Authorities: Installation of a Tracking Application

In the spring of 2025, Russian authorities enacted a law replacing the migration registration requirement for several categories of foreign citizens with the mandatory installation of a

---

Rules for Mandatory Certification of Technical Equipment for Ensuring Transport Security), https://base.garant.ru/71500596/ [accessed November 27, 2025].

[89] See Resolution of the Government of the Russian Federation No. 156 dated February 13, 2025 "О внесении изменений в постановление Правительства Российской Федерации от 27 мая 2021 г. N 810" (On Amendments to Russian Government Resolution No. 810, dated May 27, 2021), https://www.consultant.ru/document/cons_doc_LAW_499251/ [accessed November 27, 2025].

[90] See Order of the Ministry of Transport of Russia No. 162 dated May 2, 2024 "Об утверждении порядка формирования и ведения автоматизированных централизованных баз персональных данных о пассажирах и персонале (экипаже) транспортных средств, а также срока хранения и порядка предоставления содержащихся в них данных" (On the Approval of the Procedure for the Creation and Maintenance of Automated Centralized Databases of Personal Data on Passengers and Personnel (Crew) of Transport Vehicles, as well as the Storage Period and Procedure for Providing the Data Contained Therein), https://www.consultant.ru/document/cons_doc_LAW_477721/ [accessed November 27, 2025].

[91] Meduza, "Мишустин предоставил ФСБ круглосуточный удаленный доступ к базам данных агрегаторов такси" [Mishustin Has Granted the FSB 24/7 Remote Access to Taxi Aggregator Databases]. *Meduza*, July 7, 2023, https://meduza.io/news/2023/07/07/mishustin-predostavil-fsb-kruglosutochnyy-udalennyy-dostup-k-bazam-dannyh-agregatorov-taksi [accessed October 2, 2025].

[92] Dina Alimova, "Депутаты Госдумы предлагают проводить видеосъемку поездок в такси" [State Duma Deputies Propose Implementing Video Recording in Taxi Rides]. *Legal Portal GARANT.RU,* November 11, 2024, https://www.garant.ru/news/1770251/ [accessed August 24, 2025].

geolocation tracking app as an "experimental" measure.[93] Effective September 1, 2025, the requirement to install this app, dubbed "*AMINA,*" was extended to the following categories of foreign citizens arriving visa-free in Moscow and the Moscow region: (1) citizens of Azerbaijan, Ukraine, Tajikistan, Uzbekistan, Moldova, and Georgia arriving for work purposes under a patent; (2) citizens of Kyrgyzstan, Kazakhstan, and Armenia arriving for work and exempt from obtaining a work permit or patent; (3) those arriving for periods exceeding 90 days; and (4) those who have changed the purpose of their visit.[94] Among these categories, the requirement to install the app excludes citizens of Belarus, minors, and employees of diplomatic or consular missions. This new surveillance program exemplifies the growing interconnectedness of internet and phone surveillance with the tracking of physical movements and locations. It is highly likely that authorities plan to expand this surveillance program to other categories of foreign citizens and regions in the future.

Before the 2025 amendments, foreign citizens were required to be registered by migration authorities within a specified period after entry—ranging from seven to, in rare cases, 90 days—depending on their citizenship and the purpose of their visit. Migration registration data served as the primary formal mechanism for monitoring the movement of foreign citizens.[95] This data was submitted to several information systems, the main ones being *the Central Database for the Registration of Foreign Citizens and Stateless Persons*[96] and *the MIR*.[97] These databases enabled police officers to identify individuals who either failed to register within the required timeframe or overstayed their permitted stay. At the same time, the sale of fictitious migration registration documents, living outside the registered place of residence, and frequent changes of residence addresses were widespread in Russia.

The geolocation tracking program complements video surveillance and internet activity monitoring systems by enabling precise, real-time location tracking of foreign citizens and mapping their movements without relying on video cameras. To prevent SIM card swapping, the purchase of unregistered SIM cards, and the use of multiple mobile phones, Russian authorities have implemented the measures described above. These measures require mobile operators to link SIM cards to specific phones and then associate both the SIM cards and phones with individual foreign citizens.

---

[93] See Federal Law No. 121-FZ dated May 23, 2025 "О внесении изменений в отдельные законодательные акты Российской Федерации и о проведении эксперимента по внедрению дополнительных механизмов учета иностранных граждан" (On Amendments to Certain Legislative Acts of the Russian Federation and the Implementation of an Experiment to Introduce Additional Mechanisms for Registering Foreign Citizens), https://www.consultant.ru/document/cons_doc_LAW_505834/ [accessed November 29, 2025].

[94] See paragraph 3 of the article 5 *Ibid.*

[95] See article 5 of the Federal Law No. 109-FZ dated July 18, 2006 "О миграционном учете иностранных граждан и лиц без гражданства в Российской Федерации" (On Migration Registration of Foreign Citizens and Stateless Persons in the Russian Federation), https://www.consultant.ru/document/cons_doc_LAW_61569/ [accessed November 29, 2025].

[96] See Order of the Ministry of Internal Affairs of the Russian Federation, the Ministry of Foreign Affairs of the Russian Federation, the Federal Security Service of the Russian Federation, the Ministry of Economic Development and Trade of the Russian Federation and the Ministry of Information Technology and Communications of the Russian Federation No. 148/2562/98/62/25 dated March 10, 2006 No. 148/2562/98/62/25 "О ведении и использовании центрального банка данных по учету иностранных граждан и лиц без гражданства, временно пребывающих и временно или постоянно проживающих в Российской Федерации" (On the Maintenance and Use of the Central Database for Recording Foreign Citizens and Stateless Persons Temporarily Staying and Temporarily or Permanently Residing in the Russian Federation), https://base.garant.ru/189312/ [accessed November 29, 2025].

[97] See Resolution of the Government of the Russian Federation No. 813 dated August 6, 2015 "Об утверждении Положения о государственной системе миграционного и регистрационного учета, а также изготовления, оформления и контроля обращения документов, удостоверяющих личность" (On Approval of the Regulation on the State System of Migration and Registration Records, as well as the Production, Processing, and Control of the Circulation of Identity Documents), https://www.consultant.ru/document/cons_doc_LAW_184040/ [accessed November 24, 2025].

If a foreign citizen begins blocking geolocation data, they will be removed from the register within three days and added to a "controlled persons" database,[98] which carries certain consequences that we will discuss below.

It is also noteworthy that, as with the surveillance system, the Moscow authorities were the primary initiators of the new program, while the development of *the "AMINA" app* was overseen by *the State Budgetary Institution "Infogorod,"* a subsidiary of *the Moscow Department of Information Technology*.

8. Migration Documents' Paperwork: Genomic Registration

On December 1, 2024, Russian authorities launched another "experiment" aimed at intensifying surveillance measures. This initiative involves expanding "genomic registration" or the collection of biological samples, as established by *the Resolution of the Government of the Russian Federation No. 1510 dated November 7, 2024*.[99] As a result, foreign citizens crossing the specified border checkpoints during the experiment—beginning December 1, 2024, at the main Moscow airports and the Orenburg Region checkpoint, and from June 30, 2025, at all Russian checkpoints—who apply for work patents, temporary residence permits (РВП), permanent residence permits (ВнЖ), or Russian citizenship at *the Multifunctional Migration Center in Sakharovo* will be required to provide DNA samples and obtain an electronic foreign citizen card.

It is noteworthy that *this resolution* itself states that foreign citizens, when applying to *the Multifunctional Migration Center* and undergoing "mandatory migration procedures," simultaneously "undergo voluntary state genomic registration" and are "required to obtain an electronic foreign citizen card."[100] However, the document does not clarify the "voluntary" nature of genomic registration, which is effectively treated as a "mandatory procedure." Furthermore, it does not establish the possibility of obtaining, for example, a temporary residence permit or permanent residence permit without completing "genomic registration." Of course, a person may choose to leave the country instead, but the same applies to obtaining the "electronic foreign citizen card," which is explicitly described as "mandatory." This ambiguous wording may be an attempt by the document's authors to create the appearance of protections for personal data, freedom, and privacy, when in fact such protections are absent. Additionally, the document lacks even a formal explanation for why Russian authorities are collecting "biological samples," especially since this procedure is required even from children as young as six years old, as well as from incapacitated individuals and the elderly.

It should also be noted that Russian federal legislation initially mandated DNA sampling only for prisoners and defendants. However, Russian authorities decided to expand this scope, and from 2025, individuals under administrative arrest are also required to provide DNA samples.[101] Foreign

---

[98] See paragraph 5 of the article 21 of the Federal Law No. 121-FZ dated May 23, 2025 "О внесении изменений в отдельные законодательные акты Российской Федерации и о проведении эксперимента по внедрению дополнительных механизмов учета иностранных граждан" (On Amendments to Certain Legislative Acts of the Russian Federation and the Implementation of an Experiment to Introduce Additional Mechanisms for Registering Foreign Citizens), https://www.consultant.ru/document/cons_doc_LAW_505834/ [accessed November 29, 2025].

[99] See Resolution of the Government of the Russian Federation No. 1510 dated November 7, 2024, "О проведении эксперимента по апробации правил и условий въезда в Российскую Федерацию и выезда из Российской Федерации иностранных граждан и лиц без гражданства" (On Conducting an Experiment to Test the Rules and Conditions for Entry into the Russian Federation and Exit from the Russian Federation by Foreign Citizens and Stateless Persons), https://www.garant.ru/products/ipo/prime/doc/410628090/ [accessed November 24, 2025].

[100] See subparagraph "b" of the paragraph 16 *Ibid.*

[101] See article 9 of the Federal Law No. 242-FZ dated December 3, 2008 "О государственной геномной регистрации в Российской Федерации" (On State Genomic Registration in the Russian Federation), https://base.garant.ru/12163758/ [accessed November 29, 2025].

citizens applying for migration documents are not formally included among those required to provide these samples, even under the new amendments. Nevertheless, as observed, Russian authorities have de facto included them. The collected data is entered into *the Federal Database of Genomic Information.*

The mass collection of DNA samples presents significant risks and potential for abuse by the state. It is no coincidence that the European Court of Human Rights has recognized the forced collection of DNA samples from individuals who have not committed serious crimes as an unacceptable interference with privacy (Gaughran v. The United Kingdom). Meanwhile, Russian authorities have not only expanded the categories of individuals subjected to compulsory or coercive DNA sampling but have also granted law enforcement agencies virtually unlimited and unsupervised access to the genomic database.[102]

It is important to note that Russia is not the only country engaged in the mass collection of DNA samples. For example, the United States has maintained a program for several decades that collects DNA samples from convicted and criminally charged individuals. Since 2020, U.S. authorities have actively expanded the Combined DNA Index System (CODIS) database to include migrants. However, three key differences between the U.S. and Russian programs should be emphasized. In the U.S.: (1) DNA samples are collected only from migrants who have been arrested or detained under U.S. authority; (2) migrants in other categories may refuse to provide samples; and (3) the program, along with abuses during its implementation, has faced significant criticism and is contested by human rights organizations and many politicians.[103]

The Russian authorities' DNA collection program closely resembles that of China. Since 2017, Chinese authorities have significantly accelerated their forced genomic registration program, which was initially launched in 2003. At first, this program—similar to Russia's—applied only to convicted and criminally charged individuals. However, in 2013, it was expanded to include the entire population of the Tibet Autonomous Region, which Chinese authorities consider prone to protests and separatism. In 2016, the registration extended to another "problematic" and much larger region, Xinjiang, home to the majority of Uyghurs. Since 2017, the program has become nationwide, and hundreds of millions of DNA samples have been collected, although the exact number remains unknown.[104]

Beyond direct criminal investigations and legitimate family kinship cases, DNA collection raises significant concerns regarding potential abuses and data breaches. Such abuses may include unauthorized identification of family relationships, ethnicity determination for targeted surveillance or repression, and research into body structure and disease predisposition aimed at compromising information, intimidation, or targeted infection. Additionally, there is indirect evidence suggesting

---

[102] Aleks Lokhmutov, "Россия легализует массовый сбор ДНК-профилей граждан" [Russia Legalizes Mass DNA Profiling of Citizens]. *Human Rights Watch*, February 9, 2023, https://www.hrw.org/ru/news/2023/02/09/russia-legalizes-massive-dna-collection-without-oversight [accessed October 8, 2025].

[103] Georgetown Law. *Raiding the Genome: How the United States Government Is Abusing Its Immigration Powers to Amass DNA for Future Policing* (Georgetown Law, 2025), https://www.law.georgetown.edu/privacy-technology-center/publications/raiding-the-genome/ [accessed October 9, 2025].

[104] Emile Dirks and James Leibold, *Genomic Surveillance. Inside China's DNA dragnet*. ASPI (Australian Strategic Policy Institute), International Cyber Policy Centre. Report No. 34, 2020, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-06/Genomic%20surveillance_1.pdf [accessed October 9, 2025].

that DNA collected in China[105]—and possibly Russia[106]—is being utilized for military research. This latter application is of particular global concern, as it involves so-called "genetic weapons" (genetic-based or biogenetic weapons), which could have horrific and unpredictable consequences.

9. Transactions, Transfers and Purchases: Financial Monitoring

If a foreign citizen wishes to open a bank account, make an international transfer, or simply purchase goods using a credit card, these actions are automatically tracked and processed. If law enforcement agencies have an interest, they conduct a thorough investigation.

Russian authorities have actively utilized banks for surveillance and control over several years, including enforcing account freezes and seizing funds. In the 2020s, they introduced numerous new regulations aimed at broadly integrating banks into a system of surveillance, control, and punishment. Five notable trends regarding banks' involvement in this surveillance system are worth highlighting. In recent years, Russian authorities have: (1) expanded the list of agencies with access to banking secrecy and control over the banking system—for example, by including tax authorities, customs officials, and prosecutors; (2) implemented measures to ensure easy, rapid, and virtually unlimited access for a wide range of government agencies to nearly all banking information; (3) restricted banks' participation in international information exchange and, in many cases, prohibited them from interacting with foreign financial institutions without direct government authorization; (4) used banks to collect biometric data; and (5) introduced mechanisms compelling banks to quickly and extrajudicially block accounts, forcibly seize funds, and collect additional data from clients in the interests of Russian authorities.[107]

In addition to banks, Russian authorities have expanded surveillance of users on online platforms for the sale and exchange of goods and services, including marketplaces and classified ads. According to new regulations, Russian marketplaces (trading platforms) and classified ads (bulletin boards) are required, upon request from law enforcement agencies—ranging from *the FSB* and t*he Ministry of Internal Affairs* to *the Russian National Guard*, and *the Federal Protective Service*—to promptly transfer data about their clients. This data includes phone numbers, email addresses, information about completed purchases and services, as well as specialized technical details about users, such as IP addresses, unique user identifiers (UIDs), mobile equipment identifiers (IMEIs), MAC addresses, and even device geolocation.[108]

All these measures apply to both Russian and foreign citizens. Regarding the latter, Russian authorities have adopted or plan to adopt several additional regulations that subject this group to even closer surveillance. For instance, in late March 2025, *Rosfinmonitoring* proposed limiting the validity of bank cards for foreign citizens to one year and introducing additional requirements for account opening. In April 2025, the *Prosecutor General's Office* endorsed the idea of increased oversight of bank transfers made by migrants.

---

[105] Joby Warrick and Cate Brown, "China's quest for human genetic data spurs fears of a DNA arms race," *The Washington Post*, September 21, 2023, https://www.washingtonpost.com/world/interactive/2023/china-dna-sequencing-bgi-covid/ [accessed August 21, 2025].

[106] Robert Petersen, "Fear and Loathing in Moscow. The Russian biological weapons program in 2022". *Bulletin of the Atomic Scientists,* Ocotber 5, 2022, https://thebulletin.org/2022/10/the-russian-biological-weapons-program-in-2022/ [accessed August 22, 2025].

[107] Roskomsvoboda, "Банкам запретили передавать данные о клиентах иностранным органам" [Banks Are Prohibited from Transferring Client Data to Foreign Authorities]. Abril 20, 2022, https://roskomsvoboda.org/en/post/delitsya-banktaynoy-nelzya/ [accessed October 9, 2025].

[108] Roskomsvoboda, "Силовики могут получить новые инструменты для слежки" [Law Enforcers May Receive New Surveillance Tools]. June 20, 2025, https://roskomsvoboda.org/en/post/marketplace-data-access-rules-update/ [accessed October 9, 2025].

10. Inclusion in the Register of Controlled Persons: Restrictions and Expulsion from Russia

According to the 2024 amendments, if the algorithms of migration information systems determine that a foreign citizen has violated migration regulations, or if *the FSB* or *the Russian MIA* revokes their migration documents for any reason, the migrant is added to *the so-called "Register of Controlled Persons"* (реестр контролируемых лиц), and an "expulsion regime" (режим высылки) is activated.[109]

Russian law enforcement agencies have long maintained lists of foreign nationals they believe have violated migration regulations. These lists were compiled using various databases and systems, the most notable being were *the Automated System of the Central Data Bank for Registration of Foreign Citizens and Stateless Persons* and *the Automated Information System "Criminal-I."* However, these lists were not formally established by law and were considered indicative rather than definitive. Inclusion on these lists served as grounds for additional checks by migration authorities but did not result in immediate sanctions. Previously, if officers identified a foreign national on the list, they would conduct a verification; if a violation of migration regulations was confirmed, the individual would be detained, and the relevant courts would determine administrative penalties and deportation. Recently, this process has changed dramatically.

In 2024, Russian authorities announced the creation of a "register of controlled persons" and enacted *Federal Law No. 260-FZ dated August 8, 2024*, which came into effect in early 2025. This registry largely explains why Russian authorities have rapidly implemented new surveillance technologies and persistently collected extensive data from foreign citizens before, during, and after their crossings of Russian border checkpoints. Inclusion in the register of controlled persons entails several restrictive measures that significantly complicate the lives of foreign citizens and are directly linked to the surveillance and control systems described above. For example, individuals on the register are prohibited from opening bank accounts or making bank transfers, denied the right to register a marriage at a civil registry office, and, if they wish to relocate and be subject to immigration control, they will not be allowed to do so at local multifunctional centers without special permission from the authorities. These measures, in accordance with established regulations, are coordinated through *the Unified System of Interdepartmental Electronic Interaction*. This demonstrates the profound centralization of information systems and the integration of non-governmental organizations alongside key government agencies.

Anyone listed on the register of controlled individuals is required to promptly report their whereabouts to the authorities, explain why they are unable to leave independently, and notify the migration authorities. If a foreign citizen fails to comply with any of these requirements, migration service operatives will search for them using the surveillance system described in our report. Once detected and detained, the foreign citizen will be immediately placed in a temporary detention center for foreign nationals (deportation facility).[110]

Additions to *the Register of Controlled Persons* can occur for several reasons, including expired stays, cruise ship passengers delayed for more than 72 hours before illegally crossing the border,

[109] See article 11 of of the Federal Law No. 260-FZ dated August 8, 2024 "О внесении изменений в отдельные законодательные акты Российской Федерации" (On Amendments to Certain Legislative Acts of the Russian Federation), https://www.consultant.ru/document/cons_doc_LAW_482512/ [accessed November 29, 2025].
[110] See Federal Law No. 260-FZ dated August 8, 2024 "О внесении изменений в отдельные законодательные акты Российской Федерации" (On Amendments to Certain Legislative Acts of the Russian Federation), https://www.consultant.ru/document/cons_doc_LAW_482512/ [accessed November 29, 2025].

and individuals convicted of criminal offenses.[111] It is important to note that both inclusion in and exclusion from the register are automated processes and do not formally imply judicial sanctions.[112] This legal framework allows for significant potential for arbitrary decisions. For example, one ground for inclusion in the register is the revocation of a residence permit (visa, temporary residence permit, or permanent residence permit). Under Russian law, both *the Russian MIA* and *the FSB* have the authority to revoke these documents without being required to provide explanations for their decisions.

For individuals added to *the Register of Controlled Persons*, a list of permissible surveillance methods is also established at the regulatory level. Following amendments to *the Federal Law "On the Legal Status of Foreign Citizens in the Russian Federation," Article 31.13* was introduced,[113] significantly expanding the powers of *the Russian MIA's* officers. The most controversial amendment authorizes these officers to enter, without judicial approval, any premises where a "controlled person resides, stays, or is actually located." Furthermore, the amendments grant *the Russian MIA's* officers the authority to obtain information and documents "necessary to exercise control over a controlled person," including banking, commercial, and tax secrets, such as the existence and numbers of bank accounts and cash flows. The vagueness of the wording is notable, as it refers not only to information about the controlled person but also to information "necessary to exercise control over a controlled person." In other words, law enforcement officers are explicitly authorized to request information about third parties and organizations as part of the broadly defined activity of "control over controlled persons."

In addition, subparagraphs "7," "8," and "9" indicate that employees of *the Russian MIA* also have the authority

> "7) Use technical means (including equipment for audio and video recording and photography) and information contained in state information systems and/or databases of government bodies.
>
> 8) Conduct direct or indirect surveillance, including the use of technical means, of a controlled person, the actions performed by the controlled person, and the activities of individuals and legal entities assisting the controlled person during their stay (residence) in the Russian Federation, in accordance with the provisions of paragraphs 15 and 16 of Article 31.1 of this Federal Law.
>
> 9) Utilize data from mobile devices, geolocation services, payment systems, and specialized automated facial recognition technologies."

It is striking how vaguely and ambiguously these provisions are formulated. However, when considering the general surveillance system described above, their scope becomes clear. These paragraphs explicitly authorize *the Russian MIA's* officers to access information entered into databases, use video cameras and facial recognition software, search for individuals on social media, infiltrate mobile devices, read correspondence, monitor other internet activities, track

---

[111] Irina Kuznetsova, "Мигрантов поставят на учет: как ужесточат контроль за приезжими в России" [Migrants Will Be Registered: How Russia Plans to Tighten Controls on Newcomers]. *GARANT.RU*, August 12, 2024, https://www.garant.ru/article/1753211/ [accessed August 21, 2025].

[112] See Resolution of the Government of the Russian Federation No. 1899 dated December 26, 2024 "О реестре контролируемых лиц" (On the Register of Controlled Persons), https://www.consultant.ru/document/cons_doc_LAW_495039/24ff1b9f8b660e53e8f0c8b4d3a99d434ce594fd/ [accessed November 30, 2025].

[113] See Federal Law No. 115-FZ dated July 25, 2002 "О правовом положении иностранных граждан в Российской Федерации" (On the Legal Status of Foreign Citizens in the Russian Federation) https://www.consultant.ru/document/cons_doc_LAW_37868/ [accessed November 30, 2025].

banking transactions and money transfers, monitor geolocation, conduct wiretaps, and more. Notably, such surveillance is expressly permitted not only with respect to “controlled individuals” but also concerning those individuals and organizations that “assist the controlled individual in their stay (residence).” Furthermore, it appears that the interpretation of the vague term “assistance” is left to the discretion of *the Russian MIA’s* officers themselves.

What is particularly noteworthy about *the Register of Controlled Persons* is that, while employing sophisticated new surveillance technologies, Russian authorities have demonstratively absolved themselves of any obligation to notify foreign citizens of their inclusion in this registry. Given the volume of data collected, providing such notification would have been a simple matter in many—and likely the vast majority—of cases. However, Russian authorities cynically determined that since a foreign citizen can verify their inclusion by making a request on *the Russian MIA* website, this alone constitutes "notification" of the foreign citizen.[114]

[114] See article 11 Federal Law No. 260-FZ dated August 8, 2024 “О внесении изменений в отдельные законодательные акты Российской Федерации” (On Amendments to Certain Legislative Acts of the Russian Federation), https://www.consultant.ru/document/cons_doc_LAW_482512/ [accessed November 29, 2025].

Conclusion

In recent years, Russian authorities have actively employed new surveillance methods and technologies to establish a comprehensive system of total surveillance. This new system comprises four main elements: repressive policies, an authoritarian power structure, advanced technologies, and restrictive regulations. These components are particularly evident in the surveillance framework targeting foreign citizens in Russia. In 2024 and 2025, Russian authorities implemented several significant regulatory changes specifically aimed at foreign nationals, expanding existing surveillance methods and introducing new measures. Consequently, in addition to enhancing general surveillance practices affecting the entire population within territories controlled by Russian authorities—such as video monitoring, internet tracking, and banking surveillance—mandatory voice sample collection, genomic registration, and the installation of geolocation tracking applications were introduced specifically for large categories of foreign citizens during 2024–2025.

As demonstrated in the report, Russian authorities seek to collect personal and biometric data from foreign citizens even before their entry into the country. This information is then used to track individuals and enhance the overall surveillance system, which is a part of the Russian authoritarian repressive apparatus. Upon entering the Russian Federation, foreign citizens' physical movements are monitored through a network of video cameras, various tracking systems, and, in some cases, a geolocation app. Their online activities are closely observed, and visits to banks, government agencies, multifunctional centers (MFCs), as well as money transfers, online purchases, taxi orders, and even food delivery service usage are all recorded in numerous databases. Russian law enforcement agencies generally have unrestricted access to these databases. If migration control systems determine that a foreign citizen has violated migration regulations, the individual is automatically placed in “expulsion mode.” Consequently, their freedom of movement, use of bank accounts, shopping, and other transactions are further restricted, and their activities are subjected to even closer monitoring.

Russian authorities are developing and deploying new surveillance technologies to increasingly control foreign citizens, while blatantly disregarding the protection of their rights. Legislation that expands existing surveillance systems and introduces new ones is contradictory and largely violates human rights. Law enforcement agencies, which already possessed excessively broad surveillance powers before the changes of the 2020s, have in recent years gained access to virtually every aspect of the lives of foreign citizens residing in territories controlled by Russian authorities. At the same time, many surveillance systems and technologies operate indiscriminately, failing to distinguish between foreign and Russian citizens. The primary objective of the Russian authorities is to maintain and strengthen their power by controlling the population, spreading aggressive propaganda, suppressing protests, and persecuting dissidents. Regarding surveillance specifically targeting foreign citizens, it cannot be ruled out that the authorities are testing new surveillance methods on foreign individuals with the potential aim of eventually applying them to Russian citizens as well.

References

Bibliography

Access, EFF, Privacy International, et. al. “The International Principles on the Application of Human Rights to Communications Surveillance”, https://necessaryandproportionate.org/principles/ [accessed November 21, 2025].

Aleksandrov, Aleksej. “В России начали широко рекламировать мессенджер Max. В чем его опасность и способен ли он стать аналогом китайского WeChat?” [In Russia, Messenger Max has been widely advertised. What are its dangers and is it possible for it to become a Chinese WeChat equivalent?]. *Current Time TV*, July 14, 2025, https://www.currenttime.tv/a/v-rossii-nachali-shiroko-reklamirovat-messendzher-max-v-chem-ego-opasnost-i-sposoben-li-on-stat-analogom-kitayskogo-wechat-/33472932.html [accessed September 4, 2025].

Alimova, Dina. 2“Депутаты Госдуto Communications Surveillance.” *Legal Portal GARANT.RU,* November 11, 2024, https://www.garant.ru/news/1770251/ [accessed August 24, 2025].

Aleksandrov, Aleksej. “В России начали широко рекламировать мессенджер Max. В чем его опасность и способен ли он стать аналогом китайского WeChat?” [In Russia, Messenger Max has been widely advertised. What are its dangers and is it possible for it to become a Chinese WeChat equivalent?]. *Current Time TV*, July 14. https://www.currenttime.tv/a/v-rossii-мы предлагают проводить видеосъемку поездок в такси” [State Duma Deputies Propose Implementing Video Recording in Taxi Rides]. *Legal Portal GARANT.RU,* November 11, 2025, https://www.garant.ru/news/1770251/ [accessed August 24, 2025].

Applebaum, Anna. *Auticracy, INC. The Dictators Who Want to Run the World.* Doubleday, 2024.

Borodikhin, Alexander. “Как устроено ‘санитарное дело’” [Corona of Evidence: How the “Sanitary Case” Is Organized]. *Mediazona*, July 7, 2021, https://zona.media/article/2021/07/07/korona-236 [accessed August 5, 2025].

Dick, Sergei, and Olga Tikhomirova. 2025. “Наказание за поиск в Сети. Какие штрафы грозят россиянам” [Punishments for Internet Searches: What Fines Russians Face]. *Deutsche Welle,* July 23 https://www.dw.com/ru/nakazanie-za-poisk-v-internete-kakie-strafy-grozat-rossianam/a-73388354 [accessed September 11, 2025].

Dietrich, Philipp. *The Key Player in Russia’s Cybersphere. What the West Needs to Know about VK Company*. German Council on Foreign Relations, 2023, https://dgap.org/en/research/publications/key-player-russias-cybersphere [accessed October 2, 2025].

Dirks, Emile, and James Leibold. *Genomic Surveillance. Inside China's DNA dragnet*. ASPI (Australian Strategic Policy Institute), International Cyber Policy Centre. Report No. 34, 2020, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-06/Genomic%20surveillance_1.pdf [accessed October 9, 2025].

Dmitriev Denis, and Liliya Yapparova. “Власти задумали сделать единую систему видеонаблюдения” [The authorities have decided to establish a unified video surveillance system]. Meduza, February 29, 2024, https://meduza.io/feature/2024/02/29/vlasti-zadumali-sdelat-edinuyu-sistemu-videonablyudeniya-kak-v-moskve-tolko-po-vsey-strane-iz-utechki-dokumentov-administratsii-prezidenta-my-uznali-kto-ee-razrabatyvaet [accessed September 15, 2025].

Dulneva, Marina. “Тинькофф и Сбербанк теперь передают биометрические данные клиентов властям” [Tinkoff and Sberbank Share Their Clients' Biometric Data with Russian Authorities]. *Meduza*, October 12, 2023,

https://meduza.io/cards/tinkoff-i-sberbank-teper-peredayut-biometricheskie-dannye-klientov-vlastyam-chem-opasno-hranenie-takih-dannyh-v-gosudarstvennoy-sisteme-i-kak-zapretit-ih-ispolzovat [accessed October 7, 2025].

Epifanova, Alena. *Deciphering Russia's 'Sovereign Internet Law.' Tightening Control and Accelerating the Splinternet.* German Council on Foreign, 2020, https://dgap.org/sites/default/files/article_pdfs/dgap-analyse_2-2020_epifanova_0.pdf [accessed October 17, 2025].

Gabdulhakov, Rashid. "(Con)trolling the Web: Social Media User Arrests, State-Supported Vigilantism and Citizen Counter-Forces in Russia." *Global Crime* 21, no. 3–4 (2020): 283–305.

Gavrylyuk, Anastasia. "Контрольная работа: городские камеры научат слышать звуки и распознавать силуэты" [Test: City Cameras Will Understand Sounds and Recognize Silhouettes]. *Forbes Russia*, February, 13, 2024.

———. "Сдутая камера: Минцифры намерено создать платформу видеонаблюдения за 2 млрд рублей" [Deflated Camera: The Ministry of Digital Development, Communications and Mass Media Wants Create a Video Surveillance Platform for 2 Billion Rubles]. Forbes Russia, January 13, 2025.

———. "Шире круг: силовики получат данные о местоположении пользователей маркетплейсов" [A Bigger Circle: Security Forces Will Have Data on the Location of Marketplace Users]. Forbes Russia, June 19, 2025.

Georgetown Law. *Raiding the Genome: How the United States Government Is Abusing Its Immigration Powers to Amass DNA for Future Policing*. Georgetown Law, 2025, https://www.law.georgetown.edu/privacy-technology-center/publications/raiding-the-genome/ [accessed October 9, 2025].

Glukhova, Natalia, and Lyubov Borisenko. "Going dark. Digital shutdowns are at an all-time high in Russia, with those in power now able to turn off mobile internet at will". *Novaya Gazeta Europe*, July 8, 2025, https://novayagazeta.eu/articles/2025/07/22/going-dark-en [accessed September 11, 2025].

Gohdes, Anita R. *Repression in the Digital Age. Surveillance, Censorship, and the Dynamics of State Violence*. Oxford University Press, 2024.

Feldstein, Steven. *The Rise of Digital Repression. How Technology Is Reshaping Power, Politics, and Resistance*. Oxford University Press, 2021.

HRW. "Living in Fear and Humiliation. Rising Xenophobic Harassment and Violence towards Central Asian Migrants in Russia." *Human Rights Watch*, March, 2025, https://www.hrw.org/sites/default/files/media_2025/04/russia0325web.pdf [accessed November 23, 2025].

———. "Disrupted, Throttled, and Blocked State Censorship, Control, and Increasing Isolation of Internet Users in Russia". *Human Rights Watch*, July, 2025, https://www.hrw.org/sites/default/files/media_2025/07/russia0725%20web.pdf [accessed November 26, 2025].

Insider, The. "VK представила 'российский WeChat': приложение получает доступ к микрофону, камере и передает данные властям. Главное о мессенджере" [VK Has Unveiled a "Russian WeChat": the App Accesses the Microphone And Camera And Shares Data With Authorities. Here Are the Key Facts About the Messenger]. *Insider*, Juny 5, 2025, https://theins.ru/news/281890 [accessed October 13, 2025].

Insikt Group. *Tracking Deployment of Russian Surveillance Technologies in Central Asia and Latin America*. Insikt Group, 2025, https://go.recordedfuture.com/hubfs/reports/ta-ru-2025-0107.pdf [accessed August 20, 2025].

IPHR and Global Diligence. *Russia's Digital Authoritarianism: the Kremlin's Toolkit.* International Partnership for Human Rights (IPHR) and Global Diligence LLP, 2023, https://iphronline.org/articles/russias-digital-authoritarianism-the-kremlins-toolkit/ [accessed November 22, 2025].

Kagermazov, Sergey and Anna Popova. “Не самый надежный мессенджер? Основные вопросы о Telegram” [Not the Most Reliable Messenger? Main Questions About Telegram]. *BBC News Russian*, June 11, 2025, https://www.bbc.com/russian/articles/c0lndgzwwn1o [accessed October 2, 2025].

Kislov, Daniil and Ernest Zhanaev. “Russia: Xenophobia and vulnerability of migrants from Central Asia.” *The Foreign Policy Centre,* December 4, 2017, https://fpc.org.uk/russia-xenophobia-vulnerability-migrants-central-asia/ [accessed August 22, 2025].

Kócsi, Bence, and Benjamin Finn. “Investigating WeChat: An introduction to social apps WeChat and Weixin.” *Reporters Without Borders*, August 12, 2024, https://safety.rsf.org/investigating-wechat-an-introduction-to-social-apps-wechat-and-weixin/ [accessed October 3, 2025].

Kohantes, Roman. “Russian Belgorod, Rostov Switch to "Whitelist" Mobile Internet, Allow Only Kremlin-Approved Sites,” *United24 Media*, November 27, 2025, https://united24media.com/latest-news/russian-belgorod-rostov-switch-to-whitelist-mobile-internet-allow-only-kremlin-approved-sites-13807 [accessed December 2, 2025].

Kovacic, Leonid. “Сделано не в Китае: как устроена система видеонаблюдения Москвы” [Not Made in China: How Moscow's Video Surveillance System Operates]. *Carnegie Moscow Center,* August 15, 2020, https://carnegie.ru/2020/08/05/ru-pub-82419 [accessed September 19, 2025].

Korzhova, Daria. “Самозапреты и отключения: власти запланировали меры по защите граждан в интернете” [Self-Prohibitions and Shutdowns: Authorities Plan Measures to Protect Citizens Online]. *Forbes Russia,* August 21, 2025.

Krolik, Aaron, Paul Mozur, and Adam Satariano. “Cracking Down on Dissent, Russia Seeds a Surveillance Supply Chain.” *The New York Times*, July 3, 2023, https://www.nytimes.com/2023/07/03/technology/russia-ukraine-surveillance-tech.html [accessed August 19, 2025].

Kuznetsova, Irina. “Мигрантов поставят на учет: как ужесточат контроль за приезжими в России” [Migrants Will Be Registered: How Russia Plans to Tighten Controls on Newcomers]. *GARANT.RU*, August 12, 2024, https://www.garant.ru/article/1753211/ [accessed August 21, 2025].

Legalov, Evgeny. “Небольшой брат. Как видеокамеры стали инструментом репрессий” [A Little Brother: How Video Cameras Became a Tool of Repression]. *Radio Svoboda*, May 7, 2024, https://www.svoboda.org/a/neboljshoy-brat-kak-videokamery-stali-instrumentom-repressiy/32932369.html [accessed September 8, 2025].

Litvin, Victoria. “Достали из бани” [Pulled Out of the Bathhouse]. *Novaya Gazeta Europe*, August 15, 2024, https://novayagazeta.eu/articles/2024/08/15/dostali-iz-bani [accessed September 26, 2025].

Lokhmutov, Aleks. “Россия легализует массовый сбор ДНК-профилей граждан” [Russia Legalizes Mass DNA Profiling of Citizens]. *Human Rights Watch*, February 9, 2023, https://www.hrw.org/ru/news/2023/02/09/russia-legalizes-massive-dna-collection-without-oversight [accessed October 8, 2025].

Lokot, Tetyana. “Be Safe or Be Seen? How Russian Activists Negotiate Visibility and Security in Online Resistance Practices.” *Surveillance & Society* 16, no. 3 (2018): 332–46.

Lyon, David. *Surveillance*. Oxford University Press, 2024.

Lysova, Tatiana. “Paradoxes of Authoritarian Mundane Surveillance: The Use of the Yandex.Eda Data Leak to Investigate the Powerful in Russia.” *Surveillance & Society* 23, no 3 (2025): 321–35.

Mahon, Anastassiya and Scott Walker. “Russia’s Digital Repression Landscape: Unraveling the Kremlin’s Digital Repression Tactics.” *Journal of Illiberalism Studie*s 4, no 3: 29–50.

Marx, Gary. *Windows into the Soul. Surveillance and Society in an Age of High Technology.* The University of Chicago Press, 2016.

Meduza. "VK перешел под контроль Газпромбанка и 'Согаза' друга Путина Юрия Ковальчука. Гендиректором VK станет сын Сергея Кириенко" [VK Has Come Under the Control of Gazprombank and Sogaz, Both Owned By Yuri Kovalchuk, a Close Associate of Vladimir Putin. Sergei Kiriyenko's Son Is Set to Become VK's CEO]. *Meduza*, December 3, 2021, https://meduza.io/feature/2021/12/03/vk-pereshel-pod-kontrol-gazprombanka-i-sogaza-druga-putina-yuriya-kovalchuka-gendirektorom-vk-stanet-syn-sergeya-kirienko [accessed October 2, 2025].

———. "Мишустин предоставил ФСБ круглосуточный удаленный доступ к базам данных агрегаторов такси" [Mishustin Has Granted the FSB 24/7 Remote Access to Taxi Aggregator Databases]. *Meduza*, July 7, 2023, https://meduza.io/news/2023/07/07/mishustin-predostavil-fsb-kruglosutochnyy-udalennyy-dostup-k-bazam-dannyh-agregatorov-taksi [accessed October 2, 2025].

———. "Мессенджер Max начнут предустанавливать на все смартфоны в России с 1 сентября" [Messenger Max Will Be Pre-installed on All Smartphones in Russia Starting September 1]. *Meduza*, August 21, 2025 https://meduza.io/news/2025/08/21/messendzher-max-stanut-predustanavlivat-na-vse-smartfony-v-rossii-s-1-sentyabrya [accessed October 2, 2025].

Memorial HRDC. "Mass detentions of migrants across Russia". *Memorial Human Rights Defence Centre*, Juny 20, 2024, https://memorialcenter.org/en/news/mass-detentions-of-migrants-across-russia [accessed September 26, 2025].

Moscow Times, The. "'Отказаться нельзя'. Гостиницы Москвы обязали подключиться с государственной системе видеослежки за гражданами" ["No Refusal." Moscow Hotels Required to Join State Citizen Video Surveillance System]. *Moscow Times*, October 19, 2022, https://www.moscowtimes.ru/2022/10/19/otkazatsya-nelzya-gostintsi-moskvi-obyazali-podklyuchitsya-s-gosudarstvennoi-sisteme-videoslezhki-za-grazhdanami-a25487 [accessed September 25, 2025].

———. "Три четверти российских регионов внедрили системы слежки за гражданами" [Three-quarters of Russian Regions Have Implemented Citizen Surveillance Systems]. *Moscow Times*, October 24, 2023, https://www.moscowtimes.ru/2023/10/24/tri-chetverti-rossiiskih-regionov-vnedrili-sistemi-slezhki-za-grazhdanami-a111011 [accessed September 22, 2025]

OVD-Info. "Как власти используют камеры и распознавание лиц против протестующих" [How Russian Authorities Are Using Cameras and Facial Recognition Against Protesters]. *OVD-Info*, February 17, 2022, https://reports.ovd.info/kak-vlasti-ispolzuyut-kamery-i-raspoznavanie-lic-protiv-protestuyushchih [accessed September 25, 2025].

OVD-Info and Roskomsvoboda. "Human Rights and New Technology in Russia." *OVD-Info and Roskomsvoboda,* March 6, 2023, https://ovd.info/en/human-rights-and-new-technology-russia?utm_source=google.com&utm_medium=organic&utm_term=%28not+set%29#1-6 [accessed November 25, 2025].

Paper, The. "Как оппозиционеров задерживают с помощью распознавания лиц. Рассказываем о московской системе 'Сфера' и ее аналоге в Петербурге" [How Opposition Activists Are Detained by Facial Recognition Technology. We Examine Moscow's "Sfera" System and Its Counterpart in St. Petersburg]. *Paper*, Juny 15, 2022, https://paperpaper.io/kak-oppozicionerov-zaderzhivayut-s-pom/ [accessed September 26, 2025].

Pearson, James S. “Defining Digital Authoritarianism.” *Philosophy & Technology* 37, no. 73 (2024), https://link.springer.com/article/10.1007/s13347-024-00754-8#Fn2 [accessed October 4, 2025].

Pei, Minxin. *The Sentinel State. Surveillance and the Survival of Dictatorship in China.* Harvard University Press, 2024.

Petersen, Julie K. *Introduction to Surveillance Studies.* Taylor & Francis Group, 2013.

Petersen, Robert. “Fear and Loathing in Moscow. The Russian biological weapons program in 2022.” *Bulletin of the Atomic Scientists,* Ocotber 5, 2022, https://thebulletin.org/2022/10/the-russian-biological-weapons-program-in-2022/ [accessed August 22, 2025].

Pozychanyuk, Valeria and Petro Mironenko. “ФСБ потребовала от интернет-сервисов онлайн-доступ к данным и переписке пользователей” [The FSB has demanded that internet service providers grant online access to users' data and correspondence]. *The Bell,* February 11, 2020, https://thebell.io/fsb-potrebovala-ot-internet-servisov-onlajn-dostup-k-dannym-i-perepiske-polzovatelej [accessed October 1, 2025].

Roskomsvoboda. “На столичную систему видеонаблюдения потратят порядка 28,5 млрд рублей” [28.5 Billion Rubles Will Be the Capital's Video Surveillance System]. November 10, 2020, https://roskomsvoboda.org/ru/66160/ [accessed September 22, 2025].

———. “В Москве хотят подключить камеры ТЦ к городской системе видеонаблюдения” [The Moscow Goverment Plans to Integrate Shopping Center Cameras into the City's Video Surveillance System]. *Roskomsvoboda*, October 20, 2021, https://roskomsvoboda.org/en/post/kamery-maski-kontrol/ [accessed September 24, 2025].

———. “Банкам запретили передавать данные о клиентах иностранным органам” [Banks Are Prohibited from Transferring Client Data to Foreign Authorities]. Abril 20, 2022, https://roskomsvoboda.org/en/post/delitsya-banktaynoy-nelzya/ [accessed October 9, 2025].

———. “Столичная мэрия заглянет в ночные клубы... через камеры видеонаблюдения” [The Capital City's Mayor's Office Will Peek into Nightclubs... through CCTV Cameras]. *Roskomsvoboda,* May 4, 2022, https://roskomsvoboda.org/en/post/podglyadet-za-nochikami/ [accessed September 24, 2025].

———. “Каждая третья камера видеонаблюдения подключена к системам распознавания” [Every Third CCTV Camera Is Connected to Facial Recognition Systems]. *Roskomsvoboda,* March 12, 2024, https://roskomsvoboda.org/en/post/kamery-bezgorod-ai/ [accessed September 22, 2025].

———. “Подключение вообще всех камер к системам Москвы – это кошмар и ужас” [Connecting All the Cameras to Moscow's Systems Is a Nightmare and a Horror]. May 20, 2024, https://roskomsvoboda.org/ru/post/video-camera-coffee-shop/ [accessed September 25, 2025].

———. “Силовики могут получить новые инструменты для слежки” [Law Enforcers May Receive New Surveillance Tools]. June 20, 2025, https://roskomsvoboda.org/en/post/marketplace-data-access-rules-update/ [accessed October 9, 2025].

———. “Петербургские видеокамеры научили распознавать этническую принадлежность” [St. Petersburg Video Cameras Have Been Programmed to Recognize Ethnicity]. *Roskomsvoboda,* August 25, 2025, https://roskomsvoboda.org/ru/post/ethnicity-detection-cctv-russia-policy/ [accessed September 26, 2025].

Rofe, Jean. “Иностранцев в РФ, не сдавших биометрию, лишат сим-карт” [Foreigners, Who Fail to Submit Biometrics, Will Be Deprived of SIM Cards]. *Deutsche Welle*, July 1, 2025, https://www.dw.com/ru/inostrancev-v-rossii-ne-sdavsih-biometriu-lisat-simkart/a-73109351 [accessed September 17, 2025].

Shearer, David R. *Stalin's Socialism. Repression and Social Order in the Soviet Union, 1924-1953.* Yale University Press, 2009.

Shestakov, Kirill. "В РФ проводят учения по отключению от зарубежного интернета" [Russia Is Conducting Exercises to Disconnect From the Foreign Internet]. *Detusche Welle*, December 6, 2024, https://www.dw.com/ru/v-rossii-provodat-ucenia-po-otkluceniu-ot-zarubeznogo-interneta/a-70989516 [accessed October 7, 2025].

Soldatov, Andrei and Irina Borogan. *The New Nobility: The Restoration of Russia's Security State and the Enduring Legacy of the KGB.* PublicAffairs, 2011.

———. *The Red Web. The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries.* PublicAffairs, 2015.

———. *Digital Surveillance and the Impact on Journalism in Russia.* Friedrich Naumann Foundation for Freedom, 2020, https://shop.freiheit.org/#!/Publikation/943 [accessed August 18, 2025].

———. *The New Iron Curtain*. The Center for European Policy Analysis (CEPA), June 7, 2022, https://cepa.org/comprehensive-reports/the-new-iron-curtain-2/ [accessed October 13, 2025].

TelecomDaily. "В 2022 число камер для ВН в РФ превысит 21 млн" [By 2022, the Number of Video Surveillance Cameras in Russia Will Exceed 21 Million Units]. *TelecomDaily,* September 30, 2022.

United Nations Human Rights Council. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression: "Surveillance and Human Rights". *United Nations Human Rights Council*, 2019, https://digitallibrary.un.org/record/3814512?ln=en&v=pdf [accessed October 15, 2025].

———. Report of the Office of the United Nations High Commissioner for Human Rights: "The Right to Privacy in the Digital Age". *United Nations Human Rights Council*, 2022, https://docs.un.org/en/A/HRC/51/17 [accessed October 13, 2025].

———. Report of the Office of the United Nations High Commissioner for Human Rights: "Human Rights and New and Emerging Digital Technologies". *United Nations Human Rights Council*, 2024, https://docs.un.org/en/A/HRC/56/45 [accessed October 13, 2025].

United Nations Human Rights Committee. 2022. Concluding Observations on the Eighth Periodic Report of the Russian Federation. *United Nations Human Rights Committee* https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=vzwD354mdCl52wdVW7BsB9KX4KJxgSe%2BTbtWWzwb2WhGmoDVuyOe3xxHoXucsUkZU%2Bn5tswtNfD%2FljU7kOdHLA%3D%3D [accessed October 13, 2025].

Ünver, H. Akin. *Artificial intelligence (AI) and human rights: Using AI as a weapon of repression and its impact on human rights*. European Parlament, 2024, https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2024)754450 [accessed November 21, 2025].

Verstka. "Власти ограничили доступ к рекордному числу сайтов в 2024 году – более чем к 417 тысячам" [Authorities Restricted Access To a Record Number of Websites in 2024—More Than 417,000]. *Verstka*, January 28, 2025, https://verstka.media/vlasti-ogranichili-dostup-k-rekordnomu-chislu-saitov-v-2024-godu-bole e-chem-k-417k-news [accessed August 20, 2025].

Warrick, Joby, and Cate Brown. "China's quest for human genetic data spurs fears of a DNA arms race". *The Washington Post*, September 21, 2023, https://www.washingtonpost.com/world/interactive/2023/china-dna-sequencing-bgi-covid/ [accessed August 21, 2025].

Weller, Toni, "The historical ubiquity of surveillance," *Histories of Surveillance from Antiquity to the Digital Era,* edited by Andreas Marklund and Laura Skouvig. Routledge, 2022.

Zakharov, Andrey. "'Умный город' или 'Старший брат'? Как мэрия научилась знать о москвичах всё" ["Smart City" or "Big Brother"? How City Hall Has Learned to Know

Everything About Muscovites]. BBC News Russian, April 10, 2020, https://www.bbc.com/russian/features-52219260 [accessed September 19, 2025].

———. “Злость, страх и силуэты. Мэрия Москвы раскрыла, какие алгоритмы распознают людей по лицам” [Anger, Fear, and Silhouettes: Moscow City Hall Has Unveiled Algorithms That Recognize Individuals by Their Facial Features.]. *BBC News Russian*, August 25, 2022, https://www.bbc.com/russian/features-62658404 [accessed September 19, 2025].

Zuckerman, Fredric S. *The Tsarist Secret Police in Russian Society, 1880-1917*. New York University Press, 1996.

Legislative acts

Decree of the President of the Russian Federation No. 622, dated October 31, 2018 “О Концепции государственной миграционной политики Российской Федерации на 2019-2025 годы” (On the Concept of the State Migration Policy of the Russian Federation for 2019–2025), https://www.consultant.ru/document/cons_doc_LAW_310139/74e338ae02b148ec31de4bc38f486b8b045d3a1e/ [accessed November 23, 2025].

Decree of the President of the Russian Federation No. 467, dated July 9, 2025 “О государственном информационном ресурсе ‘Цифровой профиль иностранного гражданина’” (On the State Information Resource “Digital Profile of a Foreign Citizen”), https://www.garant.ru/products/ipo/prime/doc/412204934/ [accessed November 24, 2025].

Decree of the President of the Russian Federation No. 738, dated October 15, 2025 “О Концепции государственной миграционной политики Российской Федерации на 2026-2030 годы” (On the Concept of the State Migration Policy of the Russian Federation for 2026–2030), https://www.garant.ru/hotlaw/federal/1887540/ [accessed November 23, 2025].

Federal Law No. 115-FZ dated July 25, 2002 “О правовом положении иностранных граждан в Российской Федерации” (On the Legal Status of Foreign Citizens in the Russian Federation), https://www.consultant.ru/document/cons_doc_LAW_37868/ [accessed November 30, 2025].

Federal Law No. 109-FZ dated July 18, 2006 “О миграционном учете иностранных граждан и лиц без гражданства в Российской Федерации” (On Migration Registration of Foreign Citizens and Stateless Persons in the Russian Federation), https://www.consultant.ru/document/cons_doc_LAW_61569/ [accessed November 29, 2025].

Federal Law No. 242-FZ dated December 3, 2008 “О государственной геномной регистрации в Российской Федерации” (On State Genomic Registration in the Russian Federation), https://base.garant.ru/12163758/ [accessed November 29, 2025].

Federal Law No. 482-FZ dated December 31, 2017 “О внесении изменений в отдельные законодательные акты Российской Федерации” (On Amendments to Certain Legislative Acts of the Russian Federation), https://www.garant.ru/products/ipo/prime/doc/71748784/ [accessed November 27, 2025].

Federal Law No. 572-FZ dated December 28, 2022 “Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации” (On the Implementation of Identification and/or Authentication of Individuals Using Biometric Personal Data, Amendments to Certain Legislative Acts of the Russian Federation, and the Recognition of Certain Provisions of Legislative Acts of the Russian Federation as Invalid), https://www.consultant.ru/document/cons_doc_LAW_436110/ [accessed November 27, 2025].

Federal Law No. 260-FZ dated August 8, 2024 “О внесении изменений в отдельные законодательные акты Российской Федерации” (On Amendments to Certain Legislative Acts of the Russian Federation),

https://www.consultant.ru/document/cons_doc_LAW_482512/ [accessed November 29, 2025].
Federal Law No. 303-FZ dated August 8, 2024 "О внесении изменений в Федеральный закон 'О связи' и отдельные законодательные акты Российской Федерации" (On Amendments to the Federal Law "On Communications" and Certain Legislative Acts of the Russian Federation), https://www.consultant.ru/document/cons_doc_LAW_482565/ [accessed November 26, 2025].
Federal Law No. 41-FZ dated April 1, 2025 "О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации" (On the Creation of a State Information System for Combating Offenses Committed Using Information and Communication Technologies, and on Amendments to Certain Legislative Acts of the Russian Federation), https://www.consultant.ru/document/cons_doc_LAW_502182/ [accessed November 26, 2025].
Federal Law No. 121-FZ dated May 23, 2025 "О внесении изменений в отдельные законодательные акты Российской Федерации и о проведении эксперимента по внедрению дополнительных механизмов учета иностранных граждан" (On Amendments to Certain Legislative Acts of the Russian Federation and the Implementation of an Experiment to Introduce Additional Mechanisms for Registering Foreign Citizens), https://www.consultant.ru/document/cons_doc_LAW_505834/ [accessed November 29, 2025].
Law of the Russian Federation No. 4730-1 dated April 1, 1993 "О Государственной границе Российской Федерации" (On the State Border of the Russian Federation), https://www.consultant.ru/document/cons_doc_LAW_3140/ [accessed November 25, 2025].
Letter of the Ministry of Digital Development of the Russian Federation No. OK-P24-58177 dated June 17, 2025 "О разъяснении правил, вводимых на территории Российской Федерации постановлением Правительства РФ от 07.11.2024 N 1510" (On Clarification of the Rules Introduced in the Territory of the Russian Federation by the Resolution of the Government of the Russian Federation No. 1510 dated November 7, 2024), https://www.consultant.ru/document/cons_doc_LAW_509343/ [accessed November 24, 2025].
Order of Roskomnadzor No. 225 dated July 31, 2019 "Об утверждении Положения о Центре мониторинга и управления сетью связи общего пользования" (On the Approval of the Regulation for the Center for Monitoring and Control of the Public Communications Network), https://www.consultant.ru/document/cons_doc_LAW_338375/5ca8c9d8a91fec8a0bb0794025b7f411b9b705f8/ [accessed November 26, 2025].
Order of the Government of the Russian Federation No. 2446-r dated December 3, 2014, "Об утверждении Концепции построения и развития аппаратно-программного комплекса 'Безопасный город'" (On Approval of the Concept for the Construction and Development of the Hardware and Software Complex "Safe City"), https://www.consultant.ru/document/cons_doc_LAW_172077/ [accessed November 25, 2025].
Order of the Ministry of Foreign Affairs of the Russian Federation No. 9175 dated May 31, 2017, "Об утверждении Порядка организации деятельности Министерства иностранных дел Российской Федерации по оформлению, выдаче, продлению срока действия визы, восстановлению либо аннулированию визы, а также порядка учета и хранения бланков виз" (On the Approval of the Procedure for Organizing the Activities of the Ministry of Foreign Affairs of the Russian Federation Regarding the Registration, Issuance, Extension of Validity, Restoration, or Cancellation of Visas, as well as the Procedure for Recording and Storing Visa Forms), https://base.garant.ru/71709404/ [accessed November 23, 2025].

Order of the Ministry of Foreign Affairs of Russia No. 22683 dated December 14, 2020 “Об утверждении состава сведений, которые указываются иностранным гражданином в заявлении об оформлении единой электронной визы, а также форм уведомлений об оформлении и об отказе в оформлении единой электронной визы” (On Approval of the Composition of Information to Be Provided by a Foreign Citizen in an Application for a Unified Electronic Visa, as well as Forms of Notifications of Issuance and Refusal to Issue a Unified Electronic Visa), https://base.garant.ru/400103460/ [accessed November 24, 2025].

Order of the Ministry of Internal Affairs of the Russian Federation, the Ministry of Foreign Affairs of the Russian Federation, the Federal Security Service of the Russian Federation, the Ministry of Economic Development and Trade of the Russian Federation and the Ministry of Information Technology and Communications of the Russian Federation No. 148/2562/98/62/25 dated March 10, 2006 No. 148/2562/98/62/25 “О ведении и использовании центрального банка данных по учету иностранных граждан и лиц без гражданства, временно пребывающих и временно или постоянно проживающих в Российской Федерации” (On the Maintenance and Use of the Central Database for Recording Foreign Citizens and Stateless Persons Temporarily Staying and Temporarily or Permanently Residing in the Russian Federation), https://base.garant.ru/189312/ [accessed November 29, 2025].

Order of the Ministry of Transport of Russia No. 162 dated May 2, 2024 “Об утверждении порядка формирования и ведения автоматизированных централизованных баз персональных данных о пассажирах и персонале (экипаже) транспортных средств, а также срока хранения и порядка предоставления содержащихся в них данных” (On the Approval of the Procedure for the Creation and Maintenance of Automated Centralized Databases of Personal Data on Passengers and Personnel (Crew) of Transport Vehicles, as well as the Storage Period and Procedure for Providing the Data Contained Therein), https://www.consultant.ru/document/cons_doc_LAW_477721/ [accessed November 27, 2025].

Resolution of the Government of the Russian Federation No. 697, dated September 8, 2010 “О единой системе межведомственного электронного взаимодействия” (On the Unified System of Interdepartmental Electronic Interaction), https://base.garant.ru/199319/ [accessed November 25, 2025].

Resolution of the Government of the Russian Federation No. 743, dated July 31, 2014, “Об утверждении Правил взаимодействия организаторов распространения информации в информационно-телекоммуникационной сети ‘Интернет’ с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации” (On Approval of the Rules for Interaction Between Organizers of Information Dissemination in the Information and Telecommunications Network “Internet” and Authorized Government Agencies Conducting Operational-Search Activities or Ensuring the Security of the Russian Federation), https://base.garant.ru/70709018/ [accessed November 11, 2025].

Resolution of the Government of the Russian Federation No. 813 dated August 6, 2015 (as amended on October 21, 2024), “Об утверждении Положения о государственной системе миграционного и регистрационного учета, а также изготовления, оформления и контроля обращения документов, удостоверяющих личность” (On Approval of the Regulation on the State System of Migration and Registration Records, as well as the Production, Processing, and Control of the Circulation of Identity Documents), https://www.consultant.ru/document/cons_doc_LAW_184040/ [accessed November 24, 2025].

Resolution of the Government of the Russian Federation No. 969 dated September 26, 2016 “Об утверждении требований к функциональным свойствам технических средств обеспечения транспортной безопасности и Правил обязательной сертификации технических средств обеспечения транспортной безопасности” (On the Approval of

Requirements for the Functional Properties of Technical Equipment Ensuring Transport Security and the Rules for Mandatory Certification of Technical Equipment for Ensuring Transport Security), https://base.garant.ru/71500596/ [accessed November 27, 2025].

Resolution of the Government of the Russian Federation No. 136 dated February 13, 2019 "О Центре мониторинга и управления сетью связи общего пользования" (On the Center for Monitoring and Control of the Public Communications Network), https://base.garant.ru/72180742/ [accessed November 26, 2025].

Resolution of the Government of the Russian Federation No. 1793 dated 7 November 2020 "О порядке оформления единых электронных виз и признании утратившими силу некоторых актов Правительства Российской Федерации" (On the Procedure for Issuing Uniform Electronic Visas and the Recognition of Certain Acts of the Government of the Russian Federation as Invalid), https://www.consultant.ru/document/cons_doc_LAW_367444/47e1f3ca06b495c2673ba8e2e466a0feaa84c4f8/ [accessed November 24, 2025].

Resolution of the Government of the Russian Federation No. 1510 dated November 7, 2024, "О проведении эксперимента по апробации правил и условий въезда в Российскую Федерацию и выезда из Российской Федерации иностранных граждан и лиц без гражданства" (On Conducting an Experiment to Test the Rules and Conditions for Entry into the Russian Federation and Exit from the Russian Federation by Foreign Citizens and Stateless Persons), https://www.garant.ru/products/ipo/prime/doc/410628090/ [accessed November 24, 2025].

Resolution of the Government of the Russian Federation No. 1899 dated December 26, 2024 "О реестре контролируемых лиц" (On the Register of Controlled Persons), https://www.consultant.ru/document/cons_doc_LAW_495039/24ff1b9f8b660e53e8f0c8b4d3a99d434ce594fd/ [accessed November 30, 2025].

Resolution of the Government of the Russian Federation No. 156 dated February 13, 2025 "О внесении изменений в постановление Правительства Российской Федерации от 27 мая 2021 г. N 810" (On Amendments to Russian Government Resolution No. 810, dated May 27, 2021), https://www.consultant.ru/document/cons_doc_LAW_499251/ [accessed November 27, 2025].

Resolution of the Moscow Government No. 328-PP dated March 17, 2021 "О государственной автоматизированной информационной системе 'Сфера'" (On the State Automated Information System "Sfera"), https://base.garant.ru/400484831/ [accessed November 25, 2025].

Resolution of the Moscow Government No. 47-PP dated January 21, 2025 "О внесении изменений в постановления Правительства Москвы от 16 июня 2011 г. N 272-ПП и от 19 мая 2015 г. N 299-ПП" (On Amendments to the Moscow Government Resolutions dated June 16, 2011, No. 272-PP, and May 19, 2015, No. 299-PP), https://www.consultant.ru/law/review/209259861.html [accessed November 25, 2025].