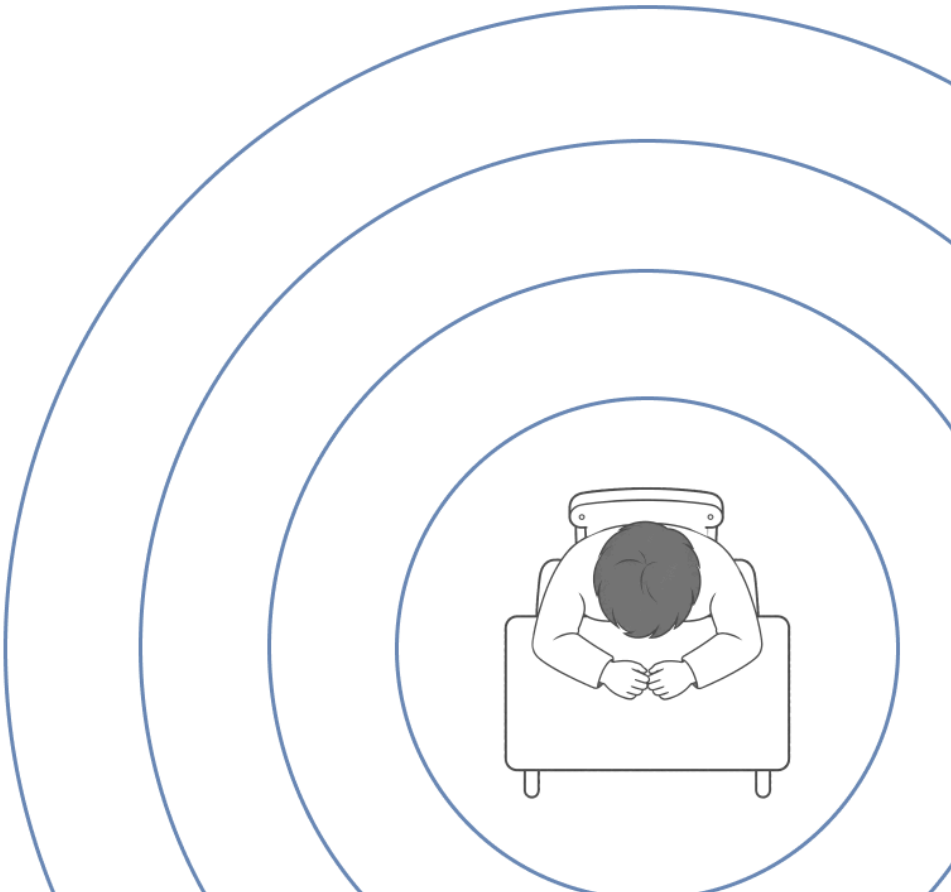
MEMORIAL
HUMAN RIGHTS DEFENCE CENTRE

POLICY REPORT | 2026

Four Perimeters of Digital Surveillance in Russian Schools

From Profiling and Video Analytics to Encryption Certificates and Cyber Squads

Konstantin Troitskiy
author of the report

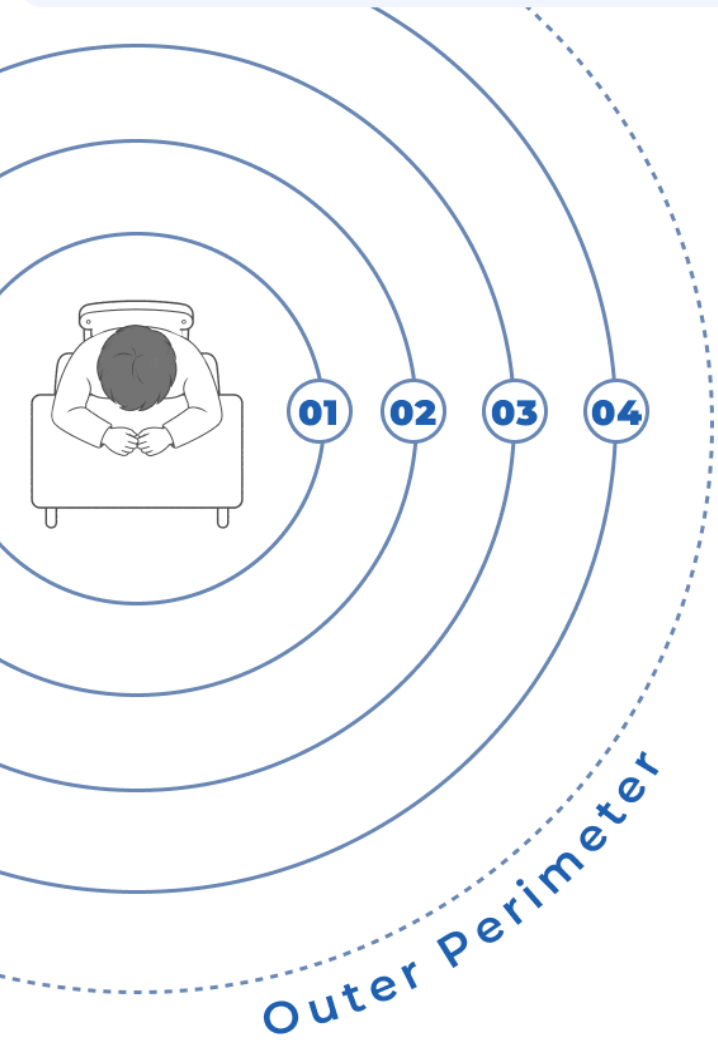


Contents

Introduction....4
Foundations of Digital Surveillance in Schools....10
Perimeter 1. FGIS "My School"....15
Data Collection and Student Profiling....15
School Communications: Sferum and Max....17
Integration into the Unified State Digital Architecture....19
Perimeter 2. Video and Audio Surveillance....22
Access Control and Biometrics....22
Cameras and Microphones....22
Video Analytics Projects....25
Perimeter 3. School Computers and Networks....29
School Network Centralization....29
Content Filtering and Federal Control over School Computers....31
Restricting Personal Devices....32
Perimeter 4. Monitoring Out-of-School Online Activity....34
School Social Media Surveillance....34
Cyber Squads....39
Neural Network Systems of Federal Agencies....40
Auxiliary Perimeters under Construction....44
Kids' SIM Cards and Control of Mobile Communications....44
Location Tracking....46
"Empathetic" Chatbots and "Soul Analytics"....47
Central Control Room....49
Conclusion....50
Sources Cited....52
Bibliography....52
Documents and materials of Russian state authorities and municipal institutions....60

Four Perimeters of Digital Surveillance

Report Structure



01 FGIS “My School”

- Student Profiling
- Sferum and Max
- Integration into State Digital Architecture

02 Video and Audio Surveillance

- Access Control and Biometrics
- Cameras and Microphones
- Video Analytics

03 School Computers and Networks

- Network Centralization
- Content Filtering
- Restrictions on Personal Devices

04 Monitoring Out-of-School Online Activity

- School Social Media Surveillance
- Cyber Squads
- Federal AI Systems and Record-Keeping

Outer Perimeter

- Kids’ SIM Cards
- Location Tracking
- Chatbots
- Central Control Room

Introduction

In the first decade of the 21st century, many experts, educators, and parents welcomed the spread of digital technologies in schools, including those that would later become tools of surveillance.[1] They hoped that these innovations would improve the quality of education and lay the foundation for a more just, free, and peaceful global community. Similarly, many pro-democracy and civil society advocates ardently supported the expansion of the internet, mobile communications, and new media, expecting such resources to provide access to reliable information, foster critical thinking, and strengthen respect for human rights among schoolchildren worldwide. But these early aspirations were soon overshadowed by the negative effects of classroom digitalization, frequent instances of outright abuse, and the danger of cutting-edge tech slipping out of human control. Moreover, authoritarian regimes—which view children as resources for their own self-preservation—have adapted these same systems to create unprecedentedly effective mechanisms of subjugation. The most notable example is China, whose use of advanced technologies in schools for social engineering has drawn criticism in democratic countries,[2] while being emulated by dictatorial states, including Russia.[3]

The Russian authorities' perception of children as convenient material for maintaining regime stability is deeply rooted in the Soviet era, which established an all-pervasive school system characterized by ideological surveillance, indoctrination, and repression.[4] The Pioneer and Komsomol organizations, state-backed denunciations, strict supervision of the educational process, a unified curriculum, and invasive propaganda were just a few components of this system. Many researchers underestimate the effectiveness of Soviet social engineering, citing its failure to prevent the collapse of the USSR. However, they overlook the fact that Soviet schools molded the key figures of the current Russian regime, who not only remember them with nostalgia but also seek to replicate many of their features. The effectiveness of Soviet social engineering is further demonstrated by the fact that, after a brief period of democratization in the 1990s, Russian schools quickly reverted to their totalitarian legacy and throughout the 2000s, despite the courageous resistance of some principals and teachers,[5] became a stronghold of the

[1] The report adopts the following definition: state surveillance is any routine, widespread, focused, and systematic monitoring by state bodies and their affiliated agents of individuals' personal data and behavior for the purposes of information gathering, control, and repression (cf. Lyon, David. *Surveillance*. Oxford, Oxford University Press, 2024).
[2] See, e.g., Ottinger, Lily. "China's AI Education Experiment". *ChinaTalk*, April 3, 2026. https://www.chinatalk.media/p/chinas-ai-education-experiment (Accessed: 06.08.2026); Shi, Chen and Jianhua Xu. "Surveillance Cameras and Resistance: A Case Study of a Middle School in China". *The British Journal of Criminology* 64, no. 5 (2024): 1150–1170.
[3] Notably, in early 2026, Chinese and Russian officials announced the launch of the "Years of Russian-Chinese Cooperation in Education," within the framework of which the governments of the two countries plan to hold numerous events.
[4] Kelly, Catriona. *Children's World: Growing Up in Russia, 1890-1991*. New Haven, Yale University Press, 2007.
[5] In some instances, teachers continued to resist the totalitarianization—and especially the militarization—of Russian schools even after the Russian authorities launched their full-scale war against Ukraine in February 2022

ruling reactionary group. In the 2010s and 2020s, the school system became an integral part of the state apparatus, carrying out various political tasks, including those that directly violated human rights: from election fraud and staged mass participation in pro-government rallies (known as "Putings") to the indoctrination of students and discrimination against migrant children.[6] The degradation of the school system became particularly evident after the Russian authorities launched their full-scale war against Ukraine in February 2022.[7]

Since the late 2010s, the Russian authorities have tested new digital technologies and control methods on children. These include biometric authentication, video analytics, geotracking, online activity monitoring, strict oversight of mobile device use, and, ultimately, digital profiling—a process that involves not only collecting vast amounts of data but also utilizing behavioral analytics, forecasting, and predictive scoring. Remarkably, these are the same technologies and methods that Russian officials have enthusiastically tested on migrants,[8] although the circumstances, objectives, and rhetoric differ for each group. Thus, while these technologies are deployed against foreign nationals under the banner of combating "illegal migration," when it comes to children, the state operates under the pretext of protecting minors from terrorism, suicide, drug trafficking, and sexual abuse. However, as will be demonstrated below, actual

(see, e.g., OVD-Info. *"The government's way or the highway": how the Russian authorities persecute teachers with an anti-war stance.* OVD-Info, January 30, 2025. https://reports.ovd.info/teachers (Accessed: 16.09.2026).

[6] See, e.g., Colin, Alexander. "Mr. Nobody Against Putin gives an insight into the propaganda in Russian schools". *The Conversation*, July 3, 2025. https://theconversation.com/mr-nobody-against-putin-gives-an-insight-into-the-propaganda-in-russian-schools-260162 (Accessed: 26.11.2025); Troitskiy, Konstantin. *Language Proficiency Testing for Foreign Children as a Tool of Russian Repressive Migration Policy*. Memorial Human Rights Defence Centre, 2026. https://memorialcenter.org/en/analytics/language-proficiency-testing (Accessed: 15.09.2026); Amnesty International. *"Only official sources" : Indoctrination in the Russian educational system*. Amnesty International, June 1, 2026. https://www.amnesty.org/en/wp-content/uploads/2026/06/EUR4609562026ENGLISH.pdf (Accessed: 15.09.2026).

[7] See, e.g., Meduza. «"Мы просто физически не успеваем вести свои обычные уроки". Как изменилось школьное образование в России за годы войны?» ["We simply physically do not have time to conduct our usual lessons". How school education in Russia has changed during the war years?]. *Meduza*, September 8, 2025. https://meduza.io/feature/2025/09/08/my-prosto-fizicheski-ne-uspevaem-vesti-svoi-obychnye-uroki (Accessed: 18.08.2026); Alava, Jonna. "From Patriotic Education to Militarist Indoctrination—Disciplinary Power and Silent Resistance in Russia after the Onset of the War against Ukraine". Problems of *Post-Communism* 72, no. 5 (2025): 429–440; Malgina, Anna. «"Господин Никто против Путина": как школьный педагог из Карабаша снял фильм, потрясший Запад. Интервью "Вот Так" с Павлом Таланкиным» ["Mr. Nobody against Putin": how a school teacher from Karabash made a film that shocked the West. An interview of "Vot Tak" with Pavel Talankin]. *vot-tak.tv*, June 3, 2025. https://vot-tak.tv/87052526/interviu-s-pavlom-talankinym (Accessed: 20.08.2026); Arkman, Arden. «Методичь. Как государственная пропаганда захватила российское образование — от детских садов до вузов» [Methodo-Madness. How state propaganda seized Russian education — from kindergartens to universities]. *The Insider*, October 10, 2025. https://theins.ru/obshestvo/284870 (Accessed: 20.08.2026); Amnesty International. *"Only official sources" : Indoctrination in the Russian educational system*. Amnesty International, June 1, 2026. https://www.amnesty.org/en/wp-content/uploads/2026/06/EUR4609562026ENGLISH.pdf (Accessed: 15.09.2026).

[8] Troitskiy, Konstantin. *The State Information Resource "Digital Profile of a Foreign National" and the Shaping of a New Russian Totalitarianism*. Memorial Human Rights Defence Centre, 2026. https://memorialcenter.org/uploads/Konstantin_Troitskiy_The_State_Information_Resource_Digital_Profile_of_a_Foreign_National_and_the_Shaping_of_a_New_Russian_Totalitarianism_7b9d44affa.pdf (Accessed: 15.09.2026).

practice reveals that the motives declared by officials sharply diverge from reality. But even if these measures result in a localized reduction of security risks for children—which is far from certain—this is merely a side effect of a totalitarian process aimed at establishing absolute state control over Russian schools in particular and Russian society as a whole. This model of safety through isolation and digital hyper-surveillance turns schools into something akin to modern maximum-security prisons: in such environments, the risk of physical violations may approach zero, but they are entirely unfit for the healthy and harmonious upbringing of children.

By the mid-2020s, most Russian schools had become zones of strict digital surveillance. This process failed to provoke genuine resistance within the purged political landscape, and the only coordinated verbal critique within the Russian Federation came from certain fundamentalist factions within the political elite. However, this so-called opposition to school digitalization is entirely hollow. First, it has never been principled and consistently avoids criticizing the top leadership of the Russian power structure. Second, it serves as a tool for controlled, state-sanctioned, and simulated protest. Third, it advocates hardline militarism and blatant totalitarianism. Fourth, these factions are an integral part of the very political regime they claim to oppose. And fifth, in practice, they combine archaic rhetoric with the promotion of digital propaganda (e.g., troll factories), cybersurveillance (e.g., the Safe Internet League), and advanced internet control technologies (e.g., traffic filtering, blacklists, and user deanonymization). The activities of these nomenklatura traditionalists—who, regarding education, cluster around figures like Sergei Kurginyan, Nikita Mikhalkov, and Ekaterina Mizulina; sham public organizations (GONGOs) like the Public Commissioner for the Protection of the Family (Общественный уполномоченный по защите семьи) and the All-Russian Parental Resistance (Родительское всероссийское сопротивление); militaristic, chauvinistic, and propagandist media outlets such as Octagon (Октагон), Krasnaya Vesna (Красная весна), and RIA “Katyusha” (РИА «Катюша»)—constitute an intra-elite rivalry between “reactionaries” and “technocrats” for resources and influence. While one faction focuses on ideological and substantive aspects, the other emphasizes technical and formal ones. In other words, this pseudo-opposition is not fighting to reverse the course toward total digital state control, but to ensure that this control is unambiguously led and promoted by the most repressive bodies of the Russian regime—the Federal Security Service (FSB), the Ministry of Internal Affairs (MVD), the Investigative Committee, and the Prosecutor’s Office. At the same time, despite their competition, these conventional “reactionaries” and “technocrats” are two sides of the same hybrid political system, in which one offers a surrogate answer to the question of “what,” and the other to the question of “how.” Regarding state oversight of school education, their roles are distributed such that the “reactionaries” prevail in substantive matters of standardization, indoctrination, and in determining punishment criteria and surveillance targets, while the conventional “technocrats” develop and implement the digital infrastructure to enforce these policies.

An analysis of the structure of state control over children in Russian schools reveals several foundational elements. The most important among them are:

- Unification — the standardization and disciplining of behavior.
- Indoctrination — the imposition of official ideological narratives on children, with any criticism prohibited.
- A system of rewards and punishments — a mechanism designed to incentivize those who conform to unification and internalize the ideology, while suppressing those who resist.
- Surveillance — a tool that makes it possible to evaluate, modify, and plan the application of the other three elements of control, thereby serving as their very foundation.

Of particular note is that surveillance data serves as the foundation for emerging predictive analytics systems, including students' social scoring. Consequently, predictive analytics becomes a fifth crucial element of control, directing the other elements toward the future. Given the fundamental importance of surveillance and the growing role of advanced technology within it, the digitalization of surveillance lies at the very core of this investigation.

Various media outlets, NGOs, and experts have addressed school surveillance and its new technologies. However, their emphasis has been limited to isolated components, while the phenomenon of surveillance in Russian schools—in all its complexity and interconnectedness—has largely escaped critical analysis. Researchers have overlooked several key factors, including the inception of a pervasive monitoring system in the late 2010s and the pivotal role of the digital profiling of children. Furthermore, this profiling became possible only through the deep integration of state platforms and the mandatory connection of all Russian schools to the Federal State Information System "My School," which laid the foundation for an all-absorbing data collection and data analytics architecture. Given these circumstances, it is unsurprising that a deeply concerning and dangerous trend from recent years remains unreported, namely, the increasing integration of various aspects of surveillance in Russian schools within a single, total-control metasystem.

The issue here is not data collection as such. All schools worldwide engage in this practice, a fact exploited by Russian propaganda to distract from the authorities' course toward totalitarianism and to downplay the scale of state intrusion into the private lives of children and their families. Rather, the critical questions are (1) what data is collected, (2) how it is collected, (3) who controls the process, and (4) for what purposes. The fundamental problem with the Russian school data-management lies in the following:

1. The state collects an excessive amount of data on children, ranging from cafeteria preferences and personal messages to favorite music and likes on opposition content.

2. The collection process grossly violates the rights to privacy, freedom of expression, and the freedom to seek and receive information, as well as protection from discrimination and the principle of informed consent for both children and parents.
3. In recent years, the primary responsibility for administering, aggregating, and ultimately using this data has shifted from schools and regional education officials to federal agencies, specifically *the siloviki* bloc (the MVD, the FSB, and the Prosecutor's Office), the digital censorship authorities (Mintsifry and the media regulator Roskomnadzor), and the indoctrination apparatus (the youth agency Rosmolodezh, the Ministry of Education, and the state-controlled "Movement of the First").
4. The data is used to profile children with the ultimate goal of establishing total state control over them through surveillance, indoctrination, and standardization systems, enforced by a framework of rewards and punishments. Additionally, this data is utilized to train AI models to operate even more effectively within these systems and to power predictive analytics.

This study provides an overview and does not aim to cover every type, method, or aspect of surveillance in Russian schools. Instead, it focuses on describing four perimeters of surveillance driven by modern digital technologies. While this report examines surveillance across all categories of minors, it is worth emphasizing that the Russian regime applies different levels of scrutiny to different groups. For instance, special attention is directed toward foreign children,[9] and most acutely, toward those undergoing forced Russification[10]—either after being removed from Ukraine[11] or while living in Ukrainian territories occupied by the Russian authorities.[12]

The use of digital technologies has fundamentally transformed surveillance, making it imperative to conceptually distinguish between "traditional surveillance"—which relies on direct visual or auditory contact and basic recording tools—and the tech-driven "new surveillance."[13] This does not imply that "traditional surveillance," such as the immediate supervision by teachers and administrators, has disappeared from Russian schools. Rather, it has been integrated into a digital environment, where school staff function as low-level operators and data providers for a

[9] Troitskiy, Konstantin. *Language Proficiency Testing for Foreign Children as a Tool of Russian Repressive Migration Policy*. Memorial Human Rights Defence Centre, 2026. https://memorialcenter.org/en/analytics/language-proficiency-testing (Accessed: 15.09.2026).
[10] Yale School of Public Health. *Forced Passportization in Russia-Occupied Areas of Ukraine*. New Haven, Humanitarian Research Lab at Yale School of Public Health, August 2, 2023.
[11] Meduza. «"Они могут начать противодействовать". Российские власти боятся детей, насильно вывезенных из Украины. Их пытаются «перевоспитать» и поставить под жесткий цифровой контроль» ["They may start resisting". The Russian authorities are afraid of children forcibly taken from Ukraine. They are trying to "re-educate" them and put them under tight digital control]. *Meduza*, March 11, 2024. https://meduza.io/feature/2024/03/11/oni-mogut-nachat-protivodeystvovat (Accessed: 20.08.2026).
[12] HRW. *Education under Occupation. Forced Russification of the School System in Occupied Ukrainian Territories*. Human Rights Watch, June 2024. https://www.hrw.org/sites/default/files/media_2024/06/ukraine_crd0624%20web_0.pdf (Accessed: 24.08.2026).
[13] Marx, Gary. *Windows into the Soul. Surveillance and Society in an Age of High Technology*. Chicago, The University of Chicago Press, 2016. P. 15–18.

high-tech system. For example, teachers and school administrations are now coerced into pressuring parents to create digital student profiles for their children. School staff also evaluate and input data on academic performance, behavior, and extracurricular activities into the system, while coordinating the installation of video surveillance. Furthermore, staff are tasked with instructing minors on how to use school computers, managing correspondence on the state-backed platform Sferum, organizing interactive lessons, and even monitoring students' social media activity.

The description of the surveillance perimeters is based on an analysis of the following sources:

- Russian legislation and regulatory acts;
- Presentations, plans, and statements by officials and developers;
- User manuals and technical documentation;
- Expert analyses and legal opinions;
- Media reports and investigative journalism.

This report does not delve into the technical nuances of school surveillance systems, as that topic requires more detailed and exhaustive research. Nor does it analyze all educational resources and systems, which would be too expansive for this format. While acknowledging these technical aspects and the need for further study, the following text aims to outline the functional, political, and normative components of school surveillance infrastructure, exposing its increasingly unified, totalitarian, and repressive nature.

Below is an analysis of the state surveillance system targeting children in Russian schools, which is designed to establish total digital control. At the same time, digitalization is a complex technological process that—along with distressing examples of its misuse and inspiring instances of its beneficial application—demands reflection in its own right, within the framework of human rights, ethics, and the Christian tradition of human dignity. Ultimately, this report is grounded in the conviction that while describing a specific repressive system, we must not lose sight of the broader questions that emerging technologies pose to humanity.[14]

[14] Leo XIV, Pope. *Magnifica humanitas: On Safeguarding the Human Person in the Time of Artificial Intelligence* (Encyclical Letter). May 15, 2026. The Holy See. https://www.vatican.va/content/leo-xiv/en/encyclicals/documents/20260515-magnifica-humanitas.html (Accessed: 29.09.2026).

Foundations of Digital Surveillance in Schools

There are many reasons why digital surveillance in Russian schools has reached a qualitatively new level, but four key factors stand out: (1) the use of cutting-edge technologies; (2) the construction of a state governance metasystem; (3) the introduction of mandatory digital profiling; and (4) the large-scale IT modernization of schools. All of these measures were implemented by the Russian authorities within a short period, specifically between 2019 and 2024.

1. Deployment of cutting-edge technologies

In the 21st century, the development of digital technologies not only accelerated but also largely displaced analog formats. This shift paved the way for datafication—an effort to digitize everything, including human traits, emotions, and behavior. Crucial to this transition were the advent of high-speed networks, the rapid processing of massive datasets, and the increasing complexity of system architectures, all of which served as prerequisites for the emergence of new surveillance technologies. However, the most significant advancement was the rise of artificial intelligence (AI), particularly neural networks, beginning in the 2010s. This breakthrough enabled the creation of fundamentally new platforms for collecting, storing, and processing data, which consequently laid the groundwork for modern systems of facial recognition, internet monitoring, and predictive analytics.

2. Construction of the State Governance Metasystem

Current surveillance in schools would have been impossible without the Russian authorities' deployment of a digital administration architecture, driven by the centralization and integration of numerous state information systems. While this process began years ago, the decisive impetus came from the project to create the "National Data Management System" (НСУД, or NSUD). The concept of this metasystem became widely known in 2018, when the first versions of the implementation plan were released.[15] At that time, officials announced that the basic components of the NSUD would become operational in 2021, with the unification of key state information systems scheduled for 2024.[16] Although the authorities, in their presentations and commentaries, attempted to frame the planned metasystem as a tool to streamline public interaction with state

[15] Analytical Center for the Government of the Russian Federation. «Национальная система управления данными. Концепция» (National Data Management System. Concept), Draft dated November 25, 2018, version 5.14 https://digital.msu.ru/wp-content/uploads/%D0%9D%D0%A1%D0%A3%D0%94.-%D0%9A%D0%BE%D0%BD%D1%86%D0%B5%D0%BF%D1%86%D0%B8%D1%8F_%D0%B28_25112018.pdf (Accessed: 20.04.2026).
[16] Krasnushkina, Nadezhda. «Чиновникам предписана самоцифровизация» [Self-digitization mandated for officials]. *Kommersant*, October 18, 2018; Kasmi, Elyas. «Власти собираются объединить все данные граждан и бизнеса в огромное электронное досье» [The authorities intend to combine all data of citizens and business into a huge electronic dossier]. *CNews*, November 30, 2018.

and commercial entities,[17] they made little secret that, in reality, this megaproject placed "*the primary emphasis on the interests of the state and the optimization of interagency cooperation*."[18]

The NSUD establishes uniform rules and quality standards for data management while creating a digital federal framework that centralizes hundreds of state databases and systems.[19] This architecture is built on "data marts" (витрины данных)—IT infrastructure segments that link, standardize, and distribute information among agencies on demand. By design, such a structure enables the integration of disparate networks through cross-referencing and ensures near-real-time data management without relying on a single physical repository. The NSUD also implements the concept of "master data" (эталонные данные), designating specialized agencies as the primary sources of information on Russian citizens, foreign nationals, and organizations. Data from various systems is automatically compared using verification algorithms, meaning that when discrepancies occur between providers, priority is given to the master data source. This method accelerates data harmonization, enabling the creation of unique digital profiles that integrate vast amounts of information.[20]

3. Introduction of mandatory digital profiling

From the very outset, one of the primary subprojects within the development of the NSUD was the implementation of state digital profiling (цифровое профилирование). A common misconception among Russian-speaking media outlets is that a profiling system is merely a large statistical database, and that a digital profile is simply an electronic dossier on an individual.[21] In reality, a digital profile is a unique cybernetic model of a person, while the profiling system acts as a dynamic infrastructure that continuously collects, updates, correlates, and analyzes data to influence human behavior. Through this mechanism, the system generates predictive models,

---

[17] See pages 21–24 in: Analytical Center for the Government of the Russian Federation. «Национальная система управления данными. Концепция» (National Data Management System. Concept), Draft dated November 25, 2018, version 5.14 https://digital.msu.ru/wp-content/uploads/%D0%9D%D0%A1%D0%A3%D0%94.-%D0%9A%D0%BE%D0%BD%D1%86%D0%B5%D0%BF%D1%86%D0%B8%D1%8F_%D0%B28_25112018.pdf (Accessed: 20.04.2026).

[18] Bakhur, Vladimir. «Эксперты: национальная система управления данными должна фокусироваться на пользе для бизнеса и граждан» [Experts: national data management system should focus on benefits for business and citizens]. *CNews*, November 29, 2018.

[19] In 2021, the Kommersant newspaper reported on more than 800 state information systems planned for integration within the framework of the Unified Information Platform of the National Data Management System (Galieva, Diana. «Госданные приглашают на платформу» [State data invited to the platform]. *Kommersant*, May 4, 2021).

[20] Ibid.

[21] See, e.g., Meduza. «Все иностранцы в России очень скоро окажутся под плотным контроля властей — на каждого человека составят максимально подробное досье» [All foreigners in Russia will very soon find themselves under tight control of the authorities — a most detailed dossier will be compiled on each person]. *Meduza*, January 28, 2026. https://meduza.io/cards/vse-inostrantsy-v-rossii-ochen-skoro-okazhutsya-pod-plotnym-kontrolem-vlastey-na-kazhdogo-cheloveka-sostavyat-maksimalno-podrobnoe-dosie (Accessed: 04.09.2026).

provides automated responses, and, in advanced state versions, enables full-scale algorithmic governance.[22]

Blanket digital profiling is a priority for the Russian authorities, as it provides them with unprecedented tools of control. Given this focus, it is no surprise that the 2019 NSUD rollout program prioritized "*developing a digital profile infrastructure*" as its first objective.[23] Notably, while the initial version of Russian Government Resolution No. 710 establishing the pilot project outlined seven "functional capabilities" included in the infrastructure, by mid-2026, subsequent amendments had more than tripled this list.[24]

What began as a single blueprint for a general digital profile infrastructure quickly evolved. By the early 2020s, officials had launched subprojects for Russian citizens, foreign nationals, and legal entities. The profiling of migrants, used by the authorities to test new control technologies, has progressed the fastest.[25] Nevertheless, the profiling of Russian citizens has by no means remained stagnant.

Minors are not exempt from this process. For several years now, a digital profile has been automatically created for all children whose births are registered by Russian civil registry offices (ЗАГС, or ZAGS), through the compulsory issuance of an individual insurance account number (СНИЛС, or SNILS).[26] The authorities use this number as a unique identifier for Russian citizens in their systems, thereby forming the basis of the profile (for foreign nationals, this identifier is issued by the MVD).[27] Furthermore, school enrollment is managed through the "Gosuslugi"

[22] For a brief history of profiling and reflections on its nature, see, for example, here: Bernard, Andreas. *Komplizen des Erkennungsdienstes. Das Selbst in der digitalen Kultur* [Accomplices of the Identification Service. The Self in Digital Culture]. Frankfurt am Main, S. Fischer Verlag GmbH, 2017; Goldenfein, Jake. *Monitoring Laws. Profiling and Identity in the World State*. Cambridge, Cambridge University Press, 2020.

[23] Resolution of the Government of the Russian Federation dated June 3, 2019 No. 710 (original version) «О проведении эксперимента по повышению качества и связанности данных...» (On conducting an experiment to increase the quality and connectivity of data...) https://ivo.garant.ru/#/document/77695224/paragraph/33:2 (Accessed: 17.09.2026).

[24] Resolution of the Government of the Russian Federation dated June 3, 2019 No. 710 (as amended on November 17, 2025) «О проведении эксперимента по повышению качества и связанности данных...» (On conducting an experiment to increase the quality and connectivity of data...) https://ivo.garant.ru/#/document/72262102/paragraph/9093:5 (Accessed: 17.09.2026).

[25] Learn more about Russian state digital profiling here: Troitskiy, Konstantin. *The State Information Resource 'Digital Profile of a Foreign National' and the Shaping of a New Russian Totalitarianism*. Memorial Human Rights Defence Centre, 2026. https://memorialcenter.org/uploads/Konstantin_Troitskiy_The_State_Information_Resource_Digital_Profile_of_a_Foreign_National_and_the_Shaping_of_a_New_Russian_Totalitarianism_7b9d44affa.pdf (Accessed: 15.09.2026).

[26] See paragraphs 5 and 15 of Section II of the Instructions on the Procedure for Maintaining Individual (Personalized) Records of Registered Persons here: Directive of the Ministry of Labour and Social Protection of the Russian Federation dated April 3, 2023 No. 256n «Об утверждении Инструкции о порядке ведения...» (On approval of the Instruction on the procedure for keeping...) https://www.consultant.ru/document/cons_doc_LAW_447676/ (Accessed: 21.08.2026).

[27] In 2019, the Russian authorities officially altered the nature of SNILS, paving the way for a digital profiling experiment launched that same year. As a result, among other changes, a personal account is opened and a SNILS is assigned to all Russian citizens, including those not covered by social insurance. This process occurs automatically

portal (Federal State Information System "Unified Portal of State and Municipal Services"), which strictly requires a child's SNILS for the application—a step that automatically links the minor's account to their pre-existing digital profile. Yet, the integration runs much deeper. As children enter the education system, the authorities further differentiate these records, creating a specialized student profile based on the general one. As detailed below, this student profile plays a key role in school surveillance. However, it is important to remember, however, that surveillance is not the only measure involved; profiling also encompasses behavioral analytics, predictive ratings, and algorithmic control. These processes rely on the framework of the Federal State Information System "My School," which thus constitutes the primary surveillance perimeter.

4. Large-scale IT modernization of schools

The implementation of mass state profiling in schools and the establishment of conditions for utilizing advanced surveillance technologies required the infrastructure of Russian educational institutions to be overhauled through digitalization. In the late 2010s, the authorities launched several initiatives to achieve this goal, the most significant of which was the "Digital Educational Environment" project (проект «Цифровая образовательная среда»). Overseen by the Ministry of Education and Mintsifry (Ministry of Digital Development, Communications and Mass Media), this initiative was part of the national "Education" megaproject and commenced in 2019, the same year the Russian Government began developing the NSUD and the digital profiling system.The "Digital Educational Environment" project budget exceeded 80 billion rubles (approximately $1.24 billion at the time) in federal expenditures alone. The vast majority of these funds was funneled into hardware—including computers, servers, interactive whiteboards, projectors, video cameras, and network infrastructure—providing schools with the physical foundation for a new, monolithic surveillance machine.[28] The completion of the project in 2024 facilitated the widespread deployment of the FGIS "My School," video monitoring, and centralized, restricted-access internet networks.[29] Crucially, the conclusion of the "Digital

in certain cases (such as at a child's birth). The number serves as a unique identifier for Russian citizens within state information systems. This latter aspect was introduced by adding a new purpose to the record-keeping system, which had previously focused solely on insurance: "u*se of the individual personal account insurance number for the identification and authentication of data regarding an individual when providing state and municipal services and performing state and municipal functions*" (see Federal Law of the Russian Federation dated April 1, 2019 No. 48-FZ «О внесении изменений в Федеральный закон "Об индивидуальном (персонифицированном) учете...» (On amending the Federal Law "On Individual (Personalized) Record-Keeping"...) https://www.consultant.ru/document/cons_doc_LAW_321413/3d0cac60971a511280cbba229d9b6329c07731f7/#dst100031 (Accessed: 22.08.2026).

[28] Directive of the Ministry of Education of the Russian Federation dated December 17, 2019 No. R-135 «Об утверждении методических рекомендаций...» (On approval of guidelines...) https://www.consultant.ru/document/cons_doc_LAW_340889/ (Accessed: 21.08.2026).

[29] Directive of the Ministry of Education of the Russian Federation dated December 2, 2019 No. 649 «Об утверждении Целевой модели цифровой образовательной среды» (On approval of the Target Model of the Digital Educational Environment...)

Educational Environment" project did not signify the end of infrastructure modernization, nor had school digitalization been confined solely to this initiative in the past.

https://www.consultant.ru/document/cons_doc_LAW_341443/ad8f4e028380894173b4f017a56c42b4c5e4ad54/#dst100011 (Accessed: 13.08.2026).

Perimeter 1.

FGIS “My School”

The Federal State Information System “My School” (ФГИС “Моя школа,” or FGIS “My School”) performs numerous functions, but in the context of surveillance, three aspects stand out: the accumulation of data and student profiles, the management of online communication, and integration into the unified state digital architecture.

Data Collection and Student Profiling

Before the advent of the FGIS “My School,” data collected on children was fragmented, limited, and inconsistent in format. It was not consolidated in a single location—whether a digital repository or a child’s paper file—as each school and region employed its own local methods for recording and processing information. Due to this fragmentation and lack of standardization, neither school administrations nor federal agencies possessed a detailed, data-driven description of minors.

Individual regions were the first to tackle this decentralization, with the Moscow administration leading the way. Immediately after assuming office in 2010, Mayor Sergei Sobyanin set the goal of creating an “online city” and initiated numerous projects to institute complete digital surveillance of Muscovites and migrants.[30] Child monitoring was realized through the Moscow Electronic School platform (Московская электронная школа), which largely laid the groundwork for the FGIS “My School,” designed to extend the Moscow model to all Russian schools.[31] Officials envisioned the new federal system as a centralized hub for collecting, unifying, and seamlessly processing data on all aspects of children’s school lives. Without this foundation, establishing ubiquitous digital surveillance of schoolchildren would have been technically impossible.

The FGIS “My School” collects a wide range of data that, until recently, was either lost in paper folders and reports or went unrecorded. This includes not only basic personal details, grades, and attendance, but also highly granular information. The system captures and permanently integrates into digital profiles[32] such data as precise school entry and exit times, reasons for

[30] Zakharov, Andrei. «“Умный город” или “Старший брат”? Как мэрия научилась знать о москвичах всё» [“Smart City” or “Big Brother”? How the Mayor’s Office learned to know everything about Muscovites]. *BBC News Russian,* April 10, 2020. https://www.bbc.com/russian/features-52219260 (Accessed: 17.09.2026).
[31] D-Russia. «Подписано соглашение об использовании решений “Московской электронной школы” при развитии ФГИС “Моя школа”» [A*n agreement was signed on the use of “Moscow Electronic School” solutions in the development of the FGIS “My School”*]. *D-Russia,* September 2, 2022.
[32] The list of data groups collected and processed in the unified school system was outlined by the authorities back in 2019, see Subparagraph “a” of paragraph 4.3 of the Appendix to Directive of the Ministry of Education of the

absences, completion rates for interactive surveys and assignments, online homework submissions, and the usage of educational training tools. It also records results from functional literacy assessments and career guidance tests, information about parents or guardians, and details on extracurricular activities—including participation in academic Olympiads, clubs, competitions, field trips, and summer camps.[33] Additionally, data related to the minor's personal account, school meals, benefits, and expenditures is tracked. Children's health records—containing sensitive information such as chronic illnesses, allergies, medical prescriptions, and contraindications—are linked to these digital profiles as well.[34] Furthermore, the system integrates the student's "social passport" (социальный паспорт) into the record. This includes details on the family's socioeconomic situation, housing conditions, and psychological assessment findings. It also tracks whether the minor holds a special status (e.g., orphan, ward of the state, or child with disabilities) or is on a delinquency prevention registry. Finally, as discussed at greater length in the section on Perimeter 4, the "social passport" incorporates the results of monitoring the student's online activity.

However, the information linked to student profiles is not limited to these categories. By late 2025, the authorities had launched and begun actively promoting the "Digital Psychologist" service, fully integrated into the FGIS "My School." This service enables children and their parents to book appointments and access online consultations regarding a wide range of issues and concerns. At the same time, the platform's technical design not only undermines genuine privacy but also signals that these free consultations function as a tool for the government to harvest and analyze data on minors' intimate lives. Moreover, maintaining true confidentiality would contradict the fundamental purpose of the FGIS "My School" and the broader state IT infrastructure built to unify, connect, and analyze all student data.

In practice, using the "Digital Psychologist" service requires identification through the Unified Identification and Authentication System (ЕСИА, or ESIA) via the "Gosuslugi" portal, which eliminates anonymity and links the request to the child's digital profile. Consequently, even without directly analyzing the conversations, the platform inevitably records and aggregates metadata such as the frequency of requests, their duration, the topics discussed, and the assigned specialist's credentials. Within a unified infrastructure, this information immediately becomes

---

Russian Federation dated December 2, 2019 No. 649 «Об утверждении Целевой модели цифровой образовательной среды» (On approval of the Target Model of the Digital Educational Environment...) https://www.consultant.ru/document/cons_doc_LAW_341443/ad8f4e028380894173b4f017a56c42b4c5e4ad54/#dst100011 (Accessed: 13.08.2026).

[33] The list of modules, functions, and systems of the FGIS "My School" as of mid-2026 can be found here: Methodological Document of the Ministry of Education of the Russian Federation and the Ministry of Digital Development, Communications and Mass Media of the Russian Federation, Functional Capabilities of TOR. School // Brief Description of FGIS "My School" TOR. Education for the Regions of the Russian Federation (Функциональные возможности ТОР. Школа // Краткое описание ФГИС «Моя школа» ТОР. Образование для субъектов РФ), 2026. Hosted on the official server of the Government of the Smolensk Region. https://obrpoch.admin-smolensk.ru/files/561/tor_kratko_av.pdf (Accessed: 12.09.2026).

[34] Ibid.

part of all-inclusive end-to-end analytics. Furthermore, the "Digital Psychologist" service allows the authorities to automatically parse conversation content at any time—if they are not doing so already.

Crucially, the FGIS "My School" plays a major role in unification, indoctrination, and the system of rewards and punishments for schoolchildren—an aspect that has not yet been addressed in serious research. Here, a single example suffices to demonstrate the interconnectedness of all these control elements. Specifically, the platform's digital library contains uniform ideological materials (books, videos, and audio recordings) that teachers use to design boilerplate group and individual activities for minors. Their utilization relies on digital surveillance, as the system tracks when and for how long a child opened the assigned material, as well as their performance scores if the content included practical tasks.[35] Based on these outcomes, the teacher conducts an assessment that, on the one hand, rewards or punishes students, and, on the other, remains linked to their digital profiles, potentially serving predictive forecasting and the tailoring of individual curricula.

School Communications: Sferum and Max

According to Russian Government Resolution No. 1241, dated July 13, 2022, one of the objectives of the FGIS "My School" is to "*ensure effective interaction and online communication between users,*" which encompasses a wide range of services, including chats, video calls, pedagogical channels, and online lessons.[36] This functionality was deployed on the basis of the Sferum platform—a joint project of VK and Rostelecom that from its very inception was pushed into schools through administrative leverage.[37] In 2023, Sferum was officially embedded into the FGIS "My School,"[38] and by 2025, it had become part of the Max state messenger, merging with it into a single surveillance contour.[39]

---

[35] Instruction for Working with the Universal Library of Digital Educational Content (UB TsOK), Инструкция по работе с Универсальной библиотекой цифрового образовательного контента (УБ ЦОК). Portal myschool.eduprosvet.ru (Accessed: 14.08.2026).

[36] See subparagraph (d) of paragraph 5 of the Regulation on the Federal Information System "My School" of the Resolution of the Government of the Russian Federation dated July 13, 2022 No. 1241 «О федеральной государственной информационной системе "Моя школа"...» (On the federal state information system "My School"...) https://www.consultant.ru/document/cons_doc_LAW_422207/ (Accessed: 06.08.2026).

[37] Litoy, Aleksandr. «Государство пришло в чат. Контроль над учителями, родителями и детьми» [The State has entered the chat. Control over teachers, parents, and children]. *Radio Free Europe/Radio Liberty*, November 30, 2023. https://www.svoboda.org/a/gosudarstvo-prishlo-v-chat-kontrolj-nad-uchitelyami-roditelyami-i-detjmi/32426381.html (Accessed: 17.08.2026).

[38] See paragraph 3(1) of the Resolution of the Government of the Russian Federation dated July 13, 2022 No. 1241 «О федеральной государственной информационной системе "Моя школа"...» (On the federal state information system "My School"...) https://www.consultant.ru/document/cons_doc_LAW_422207/ (Accessed: 06.08.2026).

[39] D-Russia. «Сервис для школ "Сферум" стал доступен из Max» [The "Sferum" service for schools became accessible from Max]. *D-Russia,* October 9, 2025.

It is worth recalling that the VK conglomerate, which owns the Max messenger, originated from the social network VKontakte, known since its early years for its close cooperation with Russian law enforcement agencies.[40] This partnership began long before the company came under full and direct government control in the early 2020s, when Vladimir Kiriyenko, son of the First Deputy Chief of Staff of the Russian Presidential Administration (Sergey Kiriyenko), became its CEO.[41] The development of the Max messenger was conducted in close collaboration with intelligence agencies, as evidenced by its full compatibility with the System for Operational Investigative Activities (COPM, or SORM), cryptographic certification by the FSB, and the implementation of tracking algorithms based on security service recommendations.[42] Independent experts continue to discover new vulnerabilities in the messenger and uncover hidden functionalities.[43] In September 2026, the digital security laboratory InterSecLab published a large-scale technical analysis of the Max messenger, demonstrating exactly how the application serves as a tool for sophisticated state surveillance.[44] In other words, the Russian authorities have integrated Sferum into a control architecture within which all communications of both children and adults are thoroughly moderated, analyzed, and entirely transparent to *the siloviki* and AI-driven algorithms.

---

[40] Poupin, Perrine. "Social media and state repression: The case of VKontakte and the anti-garbage protest in Shies, in Far Northern Russia". *First Monday* 26 (5) (2021); Dietrich, Philipp. *The Key Player in Russia's Cybersphere. What the West Needs to Know about VK Company.* German Council on Foreign Relations, September 20, 2023. https://dgap.org/en/research/publications/key-player-russias-cybersphere (Accessed: 18.08.2026).

[41] Meduza. «VK перешел под контроль Газпромбанка и "Согаза" друга Путина Юрия Ковальчука. Гендиректором VK станет сын Сергея Кириенко» [VK came under the control of Gazprombank and "Sogaz" of Putin's friend Yury Kovalchuk. Sergei Kiriyenko's son will 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: 19.08.2026).

[42] Aleksandrov, Alexey. «В России начали широко рекламировать мессенджер Max. В чем его опасность и способен ли он стать аналогом китайского WeChat?» [In Russia, the Max messenger has begun to be widely advertised. What is its danger and is it capable of becoming an analogue of the Chinese WeChat?]. *Current Time*, 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: 23.08.2026); Enders, Anna, Lea Horne, and Marla Rivera. *The Max Messenger: An Analysis of Russia's State-Mandated Messaging Application*. InterSecLab, September 2026.

[43] See, e.g., Belarusian Association of Journalists. «7 способов, которыми российский мессенджер Max следит за пользователями» [7 ways the Russian messenger Max tracks its users]. *Belarusian Association of Journalists*, October 7, 2025. https://baj.media/be/karysnae/max-sledit-za-polzovateljami/ (Accessed: 24.04.2026); Meduza. «Вы наверняка слышали, что "Макс" шпионит за пользователями. Но вряд ли представляете, сколько разных инструментов для слежки внедрено в мессенджер Возможно, разработчики даже использовали нейросеть для прослушки» [You have probably heard that "Max" spies on users. But you hardly imagine how many different tracking tools are implemented in the messenger. Perhaps the developers even used a neural network for wiretapping]. *Meduza*, May 22, 2026. https://meduza.io/feature/2026/05/22/vy-uzhe-navernyaka-slyshali-chto-maks-shpionit-za-svoimi-polzovatelyami-no-vryad-li-predstavlyaete-skolko-raznyh-instrumentov-dlya-slezhki-vnedreno-v-etot-messendzher (Accessed: 22.05.2026); Strelnikov, Aleksey. «Мессенджер-шпион Max? Как россияне переходят на "максофоны"» [Spy messenger Max? How Russians are switching to "maxophones"]. *Deutsche Welle*, March 23, 2026. https://www.dw.com/ru/max-messendzerspion-pocemu-rossiane-perehodat-na-maksofony/a-76494140 (Accessed: 23.04.2026).

[44] Enders, Anna, Lea Horne, and Marla Rivera. *The Max Messenger: An Analysis of Russia's State-Mandated Messaging Application*. InterSecLab, September 2026.

Integration into the Unified State Digital Architecture

Creating the FGIS "My School" as a standalone information system would have been insufficient for nationwide surveillance targeting schoolchildren. Even after standardization and consolidation on a single educational platform, student data would remain siloed from other agencies' databases and inaccessible to advanced algorithmic models. In many democratic countries, educational infrastructure is deliberately isolated from other information systems precisely to protect privacy and to prevent abuses such as the mass surveillance of minors and the creation of "digital twins" (i.e., all-encompassing, state-controlled digital profiles). However, the Russian authorities initially intended the FGIS "My School" to be an integral component of a nationwide information architecture designed for total control.

Although the FGIS "My School" was activated and officially approved in the early 2020s,[45] its development began in the late 2010s.[46] This process coincided with the deployment of the NSUD, which, as previously mentioned, served as the normative, methodological, and technological foundation for integrating hundreds of systems into a single digital state architecture. Initially, the FGIS "My School" was managed by the Ministry of Education, but under Resolution No. 1241, the Russian Government transferred it to Mintsifry.[47] At that time, the latter was already acting as the operator of the Unified Information Platform, cementing its role as the primary entity overseeing the technological aspects of the NSUD project.[48] Taken as a whole, Mintsifry functions as a pillar of Russia's state surveillance system. The activities of the Ministry and its subordinate agency, Roskomnadzor, in this sphere are extensive, ranging from the deployment of deep packet inspection (DPI)-enabled Technical Measures for Countering Threats (ТСПУ, or TSPU) and the creation of digital systems to the development of specialized software and mass network monitoring.[49]

---

[45] Mikhalchenko, Elizaveta and Kseniya Mironova. «Школа хочет все знать о семье. В цифровую образовательную среду могут быть включены персональные данные учеников, учителей и родителей» [The school wants to know everything about the family. Personal data of students, teachers, and parents may be included in the digital educational environment]. *Kommersant*, June 19, 2019; Stepanova, Yuliya and Anastasiya Gavrilyuk. «Школьникам соберут портфолио. Российских учеников снабдят цифровым профилем» [A portfolio will be compiled for school children. Russian students will be provided with a digital profile]. *Kommersant*, June 8, 2021.

[46] See Section IV of the annexes to the Directive of the Ministry of Education of the Russian Federation dated December 2, 2019 No. 649 «Об утверждении Целевой модели цифровой образовательной среды» (On approval of the Target Model of the Digital Educational Environment...) https://www.consultant.ru/document/cons_doc_LAW_341443/ad8f4e028380894173b4f017a56c42b4c5e4ad54/#dst100011 (Accessed: 13.08.2026).

[47] See Paragraph 4 of the Resolution of the Government of the Russian Federation dated July 13, 2022 No. 1241 «О федеральной государственной информационной системе "Моя школа"...» (On the federal state information system "My School"...) https://www.consultant.ru/document/cons_doc_LAW_422207/ (Accessed: 06.08.2026).

[48] See Paragraph 2 of the Resolution of the Government of the Russian Federation dated May 14, 2021 No. 733 «Об утверждении Положения о федеральной государственной информационной системе...» (On approval of the Regulations on the federal state information system...) https://www.consultant.ru/document/cons_doc_LAW_384215/ (Accessed: 14.08.2026).

[49] Litavrin, Maksim and David Frenkel. «Нейроскомнадзор. Чем пользуется РКН, чтобы следить за интернетом — и кто ему в этом помогает» [Neuroskomnadzor. What RKN uses to monitor the Internet — and who helps it in

Resolution No. 1241 also mandates that the FGIS "My School" be built on the basis of the unified GosTech platform, which serves as another important element in the push to integrate the infrastructure of various agencies.[50] Notably, the implementation of this initiative is also managed by Mintsifry, which chose Rostelecom as its contractor—the technical developer and operator of numerous surveillance mechanisms that will be mentioned more than once in this report. The monopoly of this state-controlled company was confirmed in December 2025, when officials designated it as the sole executor of the work.[51] GosTech was conceived by the authorities likewise in the late 2010s as a unified environment for creating state systems, as well as a single cloud space for the rapid exchange and analysis of data standardized within the NSUD. Consequently, since the FGIS "My School" falls under the management of Mintsifry, which also oversees GosTech, the school platform became one of the first systems to be migrated into this unified information space. However, after a swift start, the process stalled. Interagency competition, officials' concerns over data leaks, and the government's drive to deploy cutting-edge technologies led to the project being reformed in 2025, giving rise to the GosTech 2.0 concept.[52] This structural update quickly impacted the rollout of the surveillance machine.

In June and July 2026, regional education authorities and schools began widely publishing a template announcement regarding the final transition to the "My School" Standardized Cloud Solution (SCS). This process was effectively formalized retroactively at the federal level by a Russian Government resolution issued in August 2026.[53] The SCS itself is built on the GosTech platform and serves as a unified product for all Russian schools. Previously, data entered into the FGIS "My School" was channeled through various local educational systems developed within individual regions. Consequently, neither the data nor the submission interfaces and functions available to schools were fully standardized. The SCS has radically altered this status quo, marking a major step by the Russian authorities toward establishing centralized, pervasive control over the educational sphere as a whole and over schoolchildren in particular. In the

---

this]. *Mediazona*, February 8, 2023. https://zona.media/article/2023/02/08/grccc (Accessed: 10.08.2026); Agents. «Крупнейший взлом российской цензуры: как она охраняет здоровье Путина, помогает Навке, заводит досье на журналистов и разводит ботов» [The biggest hack of Russian censorship: how it protects Putin's health, helps Navka, creates dossiers on journalists, and spawns bots]. *Agents*, February 8, 2023. https://www.agents.media/tsenzura/ (Accessed: 27.04.2026).

[50] See Paragraph 5 of the Resolution of the Government of the Russian Federation dated July 13, 2022 No. 1241 «О федеральной государственной информационной системе "Моя школа"...» (On the federal state information system "My School"...) https://www.consultant.ru/document/cons_doc_LAW_422207/ (Accessed: 06.08.2026).

[51] Sizova, Nika. «"Гостех 2.0" будет работать на решениях провайдера облачных технологий Cloud.ru» ["Gostech 2.0" will run on solutions from cloud technology provider Cloud.ru]. *Vedomosti*, May 18, 2026.

[52] Petrova, Venera and Oleg Sapozhkov. «"Гостех", раз-два» ["Gostech," one-two]. *Kommersant*, September 22, 2025.

[53] Resolution of the Government of the Russian Federation dated August 1, 2026 No. 962 «О внесении изменений в постановление Правительства Российской Федерации...» (On amending the Resolution of the Government of the Russian Federation...) https://www.consultant.ru/document/cons_doc_LAW_541441/ (Accessed: 12.09.2026).

summer of 2026, twenty pilot regions adopted the SCS,[54] and the authorities clearly plan to extend it to all schools—apparently excluding Moscow and a few other federal subjects whose developed infrastructure already fully meets these unification requirements.

Without delving into the details of the GosTech 2.0 concept or the particular innovations of the SCS, one crucial point must be emphasized: the Russian regime is building a specialized big data environment that actively deploys AI technologies, including neural network-based deep analytics.[55] For schoolchildren and their parents, this essentially means that their data will not only undergo various forms of automated analysis but will also serve as training material for state-run AI models. Furthermore, predictive analytics based on student digital profiles is no longer a matter of the future but an ongoing process—a reality confirmed by presentations from the Ministry of Education and Mintsifry dedicated to the SCS.[56] Ultimately, everything points to the deep integration of the FGIS "My School" into the federal state administration architecture, merging it into a country-wide surveillance contour. This trajectory is clearly visible not only at the technical and functional levels but also at the organizational one.

[54] See, e.g., CNews. «Минцифры: приложением "Госуслуги Моя школа" пользуются более 12 млн человек» [Ministry of Digital Development: more than 12 million people use the "Gosuslugi My School" application]. *CNews*, September 1, 2026.
[55] Petrova, Venera and Oleg Sapozhkov. «"Гостех", раз-два» ["Gostech," one-two]. *Kommersant*, September 22, 2025.
[56] Memo of the Ministry of Education of the Russian Federation and the Ministry of Digital Development, Communications and Mass Media of the Russian Federation, dated 2026, Памятка: Типовое облачное решение (ТОР) «Моя школа» (Internal regulations of federal IT implementation). Hosted on the official server of the Education Department of KUGO. https://obr-ku.ru/images/Documents/TOR/%D0%A2%D0%9E%D0%A0_%D0%9C%D0%BE%D1%8F_%D1%88%D0%BA%D0%BE%D0%BB%D0%B0_%D0%9F%D0%B0%D0%BC%D1%8F%D1%82%D0%BA%D0%B0.pdf (Accessed: 12.09.2026).

Perimeter 2.

Video and Audio Surveillance

Access Control and Biometrics

The Access Control and Management System (СКУД, or SKUD) is integrated with the FGIS "My School" via regional platforms, logging the exact time a child enters and leaves the building. Typically, a SKUD installation includes a turnstile or a gate that opens when an RFID-chipped card, wristband, or key fob is tapped against a reader.[57] This data is immediately transmitted to the student's digital profile, allowing schools not only to track attendance but also to use these metrics for behavioral analytics, such as tracking lateness, early arrivals, or leaving the building during extended breaks. These RFID-based SKUDs are gradually being replaced by identification methods based on facial recognition technology, which is integrated with the Unified Biometric System (ЕБС, or EBS).[58] Although the authorities claim that biometric access is implemented strictly on a voluntary basis with parental consent, various deceptive tactics, manipulation, and intense administrative pressure have frequently been deployed since the late 2010s to extract such approvals.[59] Moreover, in many cases—primarily under the umbrella of the "Safe City" framework—facial recognition technology is used on children in schools without their parents ever being informed.

Cameras and Microphones

Thus, on the one hand, the SKUD is connected to the FGIS "My School," while on the other, it is increasingly becoming part of the overall school video surveillance infrastructure—and, more importantly, video analytics. For example, even if a school has not implemented a biometric entry system, surveillance cameras linked to facial recognition software can determine exactly who is using the card at the turnstile. Furthermore, school video cameras are installed far beyond entrances and exits; advanced AI-based algorithms can capture a wide range of parameters,

[57] Resolution of the Government of the Russian Federation dated July 13, 2022 No. 1241 «О федеральной государственной информационной системе "Моя школа"...» (On the federal state information system "My School"...) https://www.consultant.ru/document/cons_doc_LAW_422207/ (Accessed: 06.08.2026).
[58] Voronov, Aleksandr and Alexey Zhabin. «Детские лица сканируют для взрослых схем. В правительстве РФ рассказали, как может заработать биометрия в школах» [Children's faces are scanned for adult schemes. The Government of the Russian Federation explained how biometrics in schools might work]. *Kommersant,* December 3, 2025.
[59] Pozyachanyuk, Valeriya. «Операция "Детские ладошки". Зачем "Сбер" собирает биометрические данные школьников» [Operation "Children's Palms". Why "Sber" collects biometric data of school children]. *The Bell,* October 7, 2020. https://thebell.io/operatsiya-detskie-ladoshki-zachem-sber-sobiraet-biometricheskie-dannye-shkolnikov (Accessed: 09.09.2026).

including student behavior during breaks, time spent in the cafeteria, public event engagement, gait, clothing, "reprehensible" actions, and one's social circle. Although officials claim these systems are introduced for student safety, to stop fights, and to prevent bullying, the reality in Russia is that the authorities also—and likely even primarily—configure these technologies to monitor children's loyalty and their susceptibility to indoctrination. While cutting-edge AI technologies offer a vast array of capabilities, it is important to remember that the use of video analytics systems and their specific functionality depend on an educational institution's infrastructure, the sophistication of its operations centers, and local administrative policies. Thus, in a major regional hub, schools might be equipped with numerous video cameras linked to algorithms capable of determining even the mood in which a child arrived, stayed at school, and left. Conversely, in a poor rural educational institution, footage from a couple of outdated cameras might make it difficult to distinguish a first-grader from a fifth-grader.

Although the installation of video cameras in schools has a long history, the process expanded to a nationwide scale only in the late 2010s. In the summer of 2019, the Russian Government issued a resolution mandating that all schools install cameras as part of "anti-terrorist security measures for facilities (territories)."[60] In the early 2020s, under the "Digital Educational Environment" project, analog cameras in schools began to be replaced by digital HD devices capable of integrating with cloud-based metaplatforms equipped with AI-driven analytics systems.[61] Moscow once again took the lead, allocating three billion rubles in 2021 (approximately $40 million at the time) to outfit the capital's schools with high-resolution video hardware.[62] This built upon a long-standing trend, as the deployment of such tools and their connection to video analytics algorithms had begun in the capital well before federal programs were even announced. Indeed, as early as 2012, Moscow authorities had launched a project to connect all of the city's schools to the Unified Data Storage and Processing Center (ЕЦХД, or ETsKhD).[63]

To meet minimum requirements, a typical single-building school must have approximately 15 to 20 video cameras, although many educational institutions have significantly more. The total number of devices, their technical specifications, and their placement vary depending on the school and region. Current Russian regulations mandate surveillance setup at entrances and exits, along perimeter fencing, and inside buildings—in particular in corridors and communal areas, which local authorities generally interpret to include assembly halls, gymnasiums, central

[60] See Section III of the Resolution of the Government of the Russian Federation dated August 2, 2019 No. 1006 «Об утверждении требований к антитеррористической защищенности...» (On approval of requirements for anti-terrorist security...) https://www.consultant.ru/document/cons_doc_LAW_331342/ (Accessed: 30.07.2026).
[61] Directive of the Ministry of Education of the Russian Federation No. 634, Ministry of Digital Development, Communications and Mass Media of the Russian Federation No. 925 dated September 8, 2021 «Об утверждении стандарта оснащения...» (On approval of the equipment standard...).
[62] Kholupova, Kristina. «В московских школах установят тысячи видеокамер за миллиарды рублей» [Thousands of video cameras will be installed in Moscow schools for billions of rubles]. *CNews,* August 21, 2021.
[63] Resolution of the Government of Moscow, dated February 7, 2012, No. 24-PP, «Об утверждении Положения о государственной информационной системе "Единый центр хранения и обработки данных"» (On Approval of the Regulation on the State Information System Unified Center for Data Storage and Processing).

cloakrooms, and canteens.[64] Additionally, cameras are increasingly being placed on stair landings and in areas near changing rooms. Furthermore, although not yet universal, the practice of monitoring classrooms with video surveillance is becoming more widespread. This trend was largely driven by the nationwide mandate to furnish classrooms designated as State Final Examination centers with video recording setups.[65] As a result, school principals often keep these systems active not only during exams but for daily operations, gradually adding similar devices to other classrooms.

Crucially, modern cameras are often equipped with sensitive microphones, allowing audio recordings of children's conversations to be transcribed, processed, and analyzed using AI-driven algorithms. While such practices are unlikely to be widespread at present due to the complexity and high cost of these systems, the authorities deploy these tools to detect acoustic anomalies, such as bangs, explosions, sounds of panic, or predefined trigger words and screams.[66] However, it remains possible that, either in certain instances or in an experimental mode, audio streams undergo deeper analysis aimed at behavioral profiling.

Various federal agencies, local departments, and school staff members have access to live feeds and archived recordings, with the specific circle of authorized individuals determined by school administrators, regional officials, and *the siloviki*. All of this renders the confidentiality of children's data and the regulation of its processing virtually non-existent. For instance, school principals and their deputies, security personnel, and system administrators (a role often filled by computer science teachers) can view video feeds and archives; often, other staff members—such as cloakroom attendants, guards, social workers, and computer lab assistants—also have access.[67] Furthermore, school leadership usually reserves the right to grant access to specific video segments to anyone they deem necessary, acting at their own discretion and usually based

[64] Resolution of the Government of the Russian Federation dated August 2, 2019 No. 1006 «Об утверждении требований к антитеррористической защищенности...» (On approval of requirements for anti-terrorist security...) https://www.consultant.ru/document/cons_doc_LAW_331342/ (Accessed: 30.07.2026).

[65] Directive of the Ministry of Education of the Russian Federation No. 233, Federal Service for Supervision in Education and Science No. 552 dated April 4, 2023 «Об утверждении Порядка проведения государственной итоговой аттестации...» (On approval of the Procedure for conducting the state final certification...) https://www.consultant.ru/document/cons_doc_LAW_447215/ (Accessed: 24.08.2026).

[66] See, e.g., Novye Izvestiya. «"Это - не слежка": в школах Екатеринбурга впервые в России установили прослушку» ["This is not surveillance": Audio surveillance introduced in Yekaterinburg schools for the first time in Russia]. *Novye Izvestiya*, April 7, 2022.

[67] See regulatory documents from schools of various Russian regions, for example: Directive of the School Principal of the State Budgetary Educational Institution of the Republic of Dagestan "RCO" dated August 30, 2021 No. 109 «Положение о системе видеонаблюдения» (Regulations on the video surveillance system); Directive of the School Principal of the State Budgetary Educational Institution "Secondary General Education School No. 4 of Sunzha named after A.M. Kalimatov" dated September 1, 2022 No. 220/5 «Положение о системе видеонаблюдения» (Regulations on the video surveillance system); Directive of the School Principal of the Municipal Budgetary Educational Institution "Govzhinskaya Secondary General Education School" dated December 26, 2023 No. 166 «Положение о системе видеонаблюдения» (Regulations on the video surveillance system); Directive of the School Principal of the Municipal Budgetary Educational Institution "Secondary General Education School No. 4 of Tosno" dated September 2, 2024 No. 450 «Положение о системе видеонаблюдения» (Regulations on the video surveillance system).

on informal, verbal authorization.[68] But that is not all: while live feeds and recordings were previously confined to school servers and stored on isolated hard drives, the collection and processing of video data are now being actively consolidated at the regional level, following the model of the Moscow Unified Data Storage and Processing Center.

Thus, under the "Safe City" and "Safe Region" initiatives, most Russian regions have established major data storage and analytics centers that receive video feeds from schools. This enables personnel from the FSB, the MVD, and the National Guard (Rosgvardiya) to access school video footage remotely and directly from their own terminals.[69] It means that they no longer need to submit formal requests or visit educational institutions to copy video archives. School administrations are entirely excluded from this process; neither the principal nor—even less so—parents know who is accessing the recordings, which specific footage they are viewing, when, or for what purposes. However, the issue goes far beyond simplifying access for security and law enforcement agencies. Behind the scenes, vast amounts of incoming video footage serve as training data for neural networks and are continuously analyzed by AI-driven algorithms deployed at these regional centers.

Video Analytics Projects

This centralization did not occur overnight. Initially, the authorities planned to create a standalone video analytics system specifically for schools. In 2020, it was announced that, under the Digital Economy national program, the Rostec and Rusnano state corporations had secured a contract for the mass installation of video cameras in educational institutions. A key feature of the project was that the equipment would be connected to a computer vision system aptly named "Orwell." This system included, among other components, a facial recognition module developed by the Russian company NtechLab, a technology partner of Rostec.[70] By that time, NtechLab had already gained notoriety in independent media and opposition circles in the late 2010s, when Moscow authorities used its technology to launch a large-scale campaign to identify

[68] Ibid.

[69] Personnel from the FSB, the MVD, and Rosgvardia possess expanded powers within the scope of so-called "counter-terrorism activities" and almost certainly form the core of the agencies with direct access to school video systems. However, the list of agencies with such access may be broader; for instance, the Moscow Government reserves the right to decide—based on a formal request—whether to grant "*permanent, real-time access, including the ability to view live streams and archived footage and to utilize other services of the 'Unified Data Storage and Processing Center' state information system*." (see Directive of the Department of Information Technologies of the City of Moscow dated July 31, 2015 No. 64-16-241/15 «Об утверждении регламента доступа пользователей...» (On approval of the regulations for user access...).

[70] Kinyakina, Ekaterina. «Умные камеры будут следить за российскими школьниками. Системой видеонаблюдения с функцией распознавания лиц оснастят все 43 000 школ» [Smart cameras will monitor Russian school children. A video surveillance system with facial recognition function will equip all 43,000 schools]. *Vedomosti,* June 15, 2020.

and prosecute civic activists.[71] By mid-2020, the systems integrator Elvees-Neotek (affiliated with Rusnano), which was directly responsible for implementing the school surveillance project, reported that cameras had been installed in 1,608 schools across 12 regions, with plans to cover all 43,000 Russian schools by the end of 2024.[72] However, this ambitious initiative encountered several obstacles, including strong public backlash, high costs, infrastructure barriers, and a subsequent shortage of imported equipment.

Indeed, news of the mass rollout of biometric systems sparked sharp criticism from lawyers, IT experts, and parents. This prompted Rostec representatives to issue an ambiguous statement claiming that the cameras being installed did not actually feature facial recognition technology.[73] Although this declaration was evidently a subterfuge—as recognition algorithms are not embedded in the cameras themselves but are applied during video stream processing on the server—it demonstrated the authorities' concern over growing public discontent. And this was not the only instance of a strongly negative public reaction to such initiatives. In 2021, for example, following a public backlash over plans by Moscow Region authorities to launch an AI-driven pilot program to analyze schoolchildren's behavior and predict risks, regional officials were forced to abandon their idea.[74]

Beyond public opposition, the project to create a federal school video analytics system encountered a hardware-related impasse. The initial concept envisioned local data storage on servers within the schools themselves—an arrangement that did not satisfy *the siloviki* bloc due to the difficulty of obtaining rapid and remote access. Furthermore, subsequent sanctions led to a critical shortage of computing hardware and a sharp increase in the project's overall cost. Consequently, the authorities not only failed to establish a unified school video surveillance system by 2024, as evidenced, for instance, by statements from NtechLab management,[75] but they also revised their approach entirely. This shift, however, did not mean that they had abandoned the idea of video monitoring in educational institutions; rather, it signaled a tactical

[71] OVD-Info. *Как власти используют камеры и распознавание лиц против протестующих* [How the authorities use cameras and facial recognition against protesters]. OVD-Info, January 17, 2022. https://reports.ovd.info/kak-vlasti-ispolzuyut-kamery-i-raspoznavanie-lic-protiv-protestuyushchih (Accessed: 19.08.2026).
[72] Kinyakina, Ekaterina. «Умные камеры будут следить за российскими школьниками. Системой видеонаблюдения с функцией распознавания лиц оснастят все 43 000 школ» [Smart cameras will monitor Russian school children. A video surveillance system with facial recognition function will equip all 43,000 schools]. *Vedomosti,* June 15, 2020.
[73] Mediazona. «Ростех: устанавливаемые в школах камеры не предполагают технологию распознавания лиц» [Rostec: cameras installed in schools do not involve facial recognition technology]. *Mediazona*, June 16, 2020. https://zona.media/news/2020/06/16/technology (Accessed: 20.08.2026).
[74] Kasmi, Elyas. «Искусственный интеллект начинает контролировать поведение детей. Эксперимент поставят на российских школьниках» [Artificial intelligence begins to control children's behavior. The experiment will be conducted on Russian school children]. *CNews*, June 1, 2021.
[75] Roskomsvoboda. «Распознавание лиц внедрили в более чем 60 регионах России» [Facial recognition has been implemented in more than 60 regions of Russia]. *Roskomsvoboda*, October 24, 2023. https://roskomsvoboda.org/ru/post/syst-raspozn-62-region/ (Accessed: 20.08.2026).

pivot. The mandate to install video analytics systems in schools appears to have moved from the federal level to Russia's regions. In practice, this involved routing video feeds from school cameras directly to regional data storage and processing centers. Regions emulated the approach taken by Moscow authorities, who had not only established an effective video surveillance system in schools but had also implemented it with virtually no public pushback. For instance, when the Moscow mayor's office announced plans in 2020 to significantly expand predictive analytics capabilities using school video data—a move that sparked immediate parental discontent[76]—the city authorities abruptly curtailed public discussion of the experiment, and schools quietly proceeded to upgrade their equipment under the guise of modernization. Since all key data operations occur within the closed circuit of the Moscow Unified Data Storage and Processing Center, the public ultimately remains unaware of the precise nature of the analysis to which school video footage is subjected, how its results are recorded, or the exact purposes for which it is conducted.

Following the launch of the full-scale war against Ukraine by the Russian authorities in February 2022, the space for civil protest in Moscow and other Russian regions shrank dramatically. Amid ongoing repressive measures and aggressive state propaganda, resistance to the implementation of video analytics in schools diminished. Consequently, regional officials eventually ceased concealing such initiatives; instead, they began actively announcing new projects for algorithmic surveillance in educational institutions through loyal media outlets.[77] While officials typically adhere to general talking points emphasizing the need to ensure child safety, they are sometimes more candid. Two examples clearly illustrate this trend. First, the mayor of Surgut, while announcing the installation of facial-recognition-enabled cameras in 35 schools, explicitly identified the system's primary beneficiary by stating that "*all data is managed by the Ministry of Internal Affairs in real time*."[78] Second, even more revealing were the remarks made in the spring of 2026 by Svetlana Trenikhina, the Minister of Education for the Sverdlovsk Region: "*We would like to use artificial intelligence to ensure safety in our schools. Let the cameras—alongside the staff on duty—detect children's unlawful behavior and flag it. It will make things easier for us and free up our teachers to focus on more important, substantive matters*."[79] The minister did not explain what she meant by "flags" or what counted as children's

[76] Korolev, Igor. «"Ростелеком" получит от властей 10 миллиардов на постройку интернета без Facebook, "Вконтакте" и танчиков» ["Rostelecom" will receive 10 billion from the authorities to build an internet without Facebook, "VKontakte," and tank games]. *CNews*, August 3, 2020.
[77] Uchitelskaya Rossiya. «Школы Новосибирска планируют оснастить камерами с ИИ для профилактики агрессивного поведения» [Plans to equip Novosibirsk schools with AI cameras to prevent aggressive behavior]. *Uchitelskaya Rossiya*, August 29, 2024; Gasparyan, Tat. «В дагестанских школах появится Wi-Fi и умное видеонаблюдение до конца 2025 года» [Wi-Fi and smart video surveillance will appear in Dagestani schools by the end of 2025]. *Kommersant*, June 3, 2025; Petrova, Polina. «В школах Петербурга могут начать следить за поведением учеников с помощью искусственного интеллекта» [In St. Petersburg schools, they may begin to monitor students' behavior using artificial intelligence]. *Peterburgskaya Gazeta*, March 19, 2026.
[78] Doroshenko, Darya. «В школах Сургута установили умные камеры с функцией распознавания лиц» [Smart cameras with facial recognition function have been installed in Surgut schools]. *Yugorsky Snegir*, August 21, 2025.
[79] Kustov, Maksim. «В свердловских школах планируют внедрить ИИ для выявления девиантных подростков» [Sverdlovsk schools plan to introduce AI to identify deviant teenagers]. *Signal*, April 9, 2026.

“unlawful behavior.” However, such rhetoric suggests that the authorities are packing AI-driven algorithms with technical criteria for “infractions” without telling parents or the public. In some schools, datasets on such incidents, flagged by neural networks as violations, are likely already being fed into students’ digital profiles and may even now be used to compile covert social ratings.

Perimeter 3.

School Computers and Networks

Student activity on school computers has long been transparent to experienced system administrators and computer science teachers. However, until a few years ago, this oversight was limited to the educational institutions themselves.

School Network Centralization

Although many Russian schools had been connected to the internet since the 2010s, there was no unified control system in place at that time. While various requirements and guidelines regarding accessible content existed under the federal law "On Protecting Children from Information Harmful to Their Health and Development,"[80] school administrations or regional authorities typically decided independently which network equipment to purchase and how to configure and manage it.[81] Consequently, children's online activity at school—particularly when using personal mobile devices—was loosely regulated, barely monitored, and mostly invisible to federal agencies. To address this, officials decided to bring school internet access under fully centralized control. Achieving this goal turned out to be much easier for the authorities than deploying full-scale video analytics. Indeed, internet monitoring systems did not draw much public attention, and the principle of "control in exchange for convenience" proved highly effective. As a result, on the one hand, officials quietly took full control over school network traffic, while on the other, they promoted it as free, secure, and high-speed internet to attract more schoolchildren.

Once again, 2019 marked a turning point. As part of the "Digital Educational Environment" project (under the "Education" national initiative), the authorities launched a massive campaign to outfit schools with standardized infrastructure, subsequently connecting them to the Unified Data Transmission Network (ЕСПД, or ESPD).[82] Originally launched in early 2015 to monitor and secure government traffic,[83] this closed state network is isolated from the public internet by

[80] Federal Law of the Russian Federation dated December 29, 2010 No. 436-FZ «О защите детей от информации...» (On the protection of children from information...) https://www.consultant.ru/document/cons_doc_LAW_108808/ (Accessed: 12.08.2026).
[81] Kolomychenko, Mariya. «В России появится школьный реестр запрещенных сайтов» [A school registry of banned websites will appear in Russia]. *CNews*, April 17, 2014.
[82] Korolev, Igor. «"Ростелеком" получит от властей 10 миллиардов на постройку интернета без Facebook, "Вконтакте" и танчиков» ["Rostelecom" will receive 10 billion from the authorities to build an internet without Facebook, "VKontakte," and tank games]. *CNews*, August 3, 2020.
[83] Resolution of the Government of the Russian Federation, dated November 24, 2014, No. 1240, «О некоторых вопросах по обеспечению использования сети передачи данных органов власти» (On Certain Issues of

cryptographic gateways, with traffic routed through filtering nodes that render all network activity fully transparent to centralized monitoring.[84] In addition, the use of popular messaging applications such as Signal, WhatsApp, Telegram, or Viber on this network is technically impossible.

In 2019, Rostelecom—already involved in numerous state surveillance projects,[85] such as installing cameras and video analytics systems under the "Safe City" program[86]—was selected by the Russian Government as the sole contractor to connect schools to the ESPD.[87] In 2021, the authorities appointed the same state-controlled company as the sole contractor also for installing school Wi-Fi networks.[88] Meanwhile, Mintsifry, a long-standing partner of Rostelecom, was responsible for defining regulatory requirements and overseeing the entire process.[89] By the end of 2022, Rostelecom reported that all schools had been connected to the internet via the ESPD,[90] although the quality of these connections remained questionable. Indeed, a 2025 audit by the Accounts Chamber revealed that 44.6% of educational institutions did not consider their network speeds sufficient for "normal operations."[91]

Even under the initial project plan, following the rollout of the ESPD in schools, Rostelecom was required not only to ensure enhanced connection security and enforce strict content filtering—limiting access to a "whitelist" of resources mandated by the Ministry of Education as

Ensuring the Use of the Data Transmission Network of Authorities) https://www.consultant.ru/document/cons_doc_LAW_171430/ (Accessed: 12.08.2026).

[84] Directive of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation No. 417, Ministry of Education of the Russian Federation No. 221 dated April 30, 2021 «Об утверждении требований к подключению и доступу...» (On approval of requirements for connection and access...) https://www.consultant.ru/document/cons_doc_LAW_388367/2ff7a8c72de3994f30496a0ccbb1ddafdaddf518/ (Accessed: 26.08.2026).

[85] Troitskiy, Konstantin. *The State Information Resource 'Digital Profile of a Foreign National' and the Shaping of a New Russian Totalitarianism*. Memorial Human Rights Defence Centre, 2026. https://memorialcenter.org/uploads/Konstantin_Troitskiy_The_State_Information_Resource_Digital_Profile_of_a_Foreign_National_and_the_Shaping_of_a_New_Russian_Totalitarianism_7b9d44affa.pdf (Accessed: 15.09.2026).

[86] See, e.g., Samsonova, Anastasiya. «"Ростелеком" укрепился в "Безопасном городе"» ["Rostelecom" strengthened its position in "Safe City"]. *ComNews*, June 6, 2019.

[87] Resolution of the Government of the Russian Federation dated November 21, 2019 No. 2757-r «Об определении публичного акционерного общества "Ростелеком"...» (On determining the public joint-stock company "Rostelecom"...).

[88] Resolution of the Government of the Russian Federation dated March 22, 2021 No. 713-r «Об определении публичного акционерного общества "Ростелеком"...» (On determining the public joint-stock company "Rostelecom"...).

[89] Resolution of the Government of the Russian Federation, dated November 24, 2014, No. 1240, «О некоторых вопросах по обеспечению использования сети передачи данных органов власти» (On Certain Issues of Ensuring the Use of the Data Transmission Network of Authorities) https://www.consultant.ru/document/cons_doc_LAW_171430/ (Accessed: 12.08.2026).

[90] CNews. «"Ростелеком" подключил к безопасному интернету более 47 тысяч школ и техникумов» ["Rostelecom" connected more than 47 thousand schools and technical colleges to secure internet]. *CNews*, February 28, 2023.

[91] D-Russia. «Счётная палата: 44,6% школ и колледжей считают недостаточной скорость Интернета для обучения» [Accounts Chamber: 44.6% of schools and colleges consider their Internet speed insufficient for learning]. *D-Russia*, June 26, 2025.

of 2025[92]—but also to log user search queries, create "user profiles," and record attempts to access blocked sites.[93] Since authentication on school networks occurs through the "Gosuslugi" portal (specifically the ESIA system, which was also primarily developed by Rostelecom), anonymous network access is impossible.

Content Filtering and Federal Control over School Computers

The authorities went even further regarding school computers—a category that encompasses everything from desktop PCs to laptops and tablets. To bypass website encryption (HTTPS) and gain visibility into minors' network activity, Rostelecom employed a traffic interception technology based on HTTPS inspection, specifically using a "man-in-the-middle" approach. The provider required school system administrators to install a special state-issued root encryption certificate on all internet-connected school devices, thereby routing traffic through a specialized proxy server.[94] As a result, Rostelecom gained the technical capability to decrypt secure HTTPS connections in web browsers and effectively view the internet from the students' perspective, logging all web activity—from search queries and forum comments to post likes and video views—into its monitoring databases.

Yet, even after introducing all these control mechanisms, the authorities still faced a major obstacle to establishing total surveillance over children's online activity: minors could still access independent web resources and applications—even within school networks—using their own devices, which had not been turned into state surveillance tools. To overcome this hurdle, the Russian regime is deploying a multi-pronged strategy. In addition to school-specific measures—namely connecting educational organizations to the ESPD and installing state-issued root encryption certificates on computers—and broader mechanisms encompassing the entire Russian population, such as deepening federal network monitoring, further expanding SORM, and tightening internet censorship, other distinct methods of surveillance are being developed specifically targeting children. These include, first, the focused monitoring of the online environments frequented by minors; second, the introduction of so-called "kids' SIM cards"; and third, legal restrictions on the use of personal gadgets in schools. While the first two approaches are discussed in subsequent sections, the third warrants closer examination here, as it is directly linked to the authorities' efforts to compel children to use only state-provided networks, computers, messengers, and online resources.

---

[92] Official Communication of the Ministry of Education of the Russian Federation, dated November 14, 2025, «О разрешенном перечне интернет-ресурсов для использования в образовательном процессе» (On the Approved List of Internet Resources for Use in the Educational Process) https://www.consultant.ru/document/cons_doc_LAW_518910/ (Accessed: 25.08.2026).

[93] Korolev, Igor. «"Ростелеком" получит от властей 10 миллиардов на постройку интернета без Facebook, "Вконтакте" и танчиков» ["Rostelecom" will receive 10 billion from the authorities to build an internet without Facebook, "VKontakte," and tank games]. *CNews*, August 3, 2020.

[94] Rostelecom's requirement to install "root certificates" for connecting to the ESPD is outlined in the support section of this state-owned company's official website.

Restricting Personal Devices

Restricting mobile phone use in schools is a common practice worldwide. Consequently, when Russian officials enacted a legal prohibition on mobile phone use during lessons in 2023, few objected to the measure.[95] However, the details of this reform demonstrate that the Russian authorities are merely hiding behind a feigned concern for children's welfare, while their primary motive is to suppress students' digital independence and to establish total centralized state control over their online activities. At first glance, this claim might seem like a conspiracy theory surrounding this specific regulation, yet several facts support this interpretation:

1. Restrictions on gadgets were already widespread in Russian schools before the 2020s. School administrations and parent committees were empowered to codify these rules in internal bylaws without federal intervention—a practice many schools had already adopted.[96]
2. Two significant steps preceded the 2023 law. In 2021, the Federal Service for the Oversight of Consumer Protection and Welfare (Rospotrebnadzor)—under new sanitary regulations (SP 2.4.3648-20)—prohibited the school use of personal smartphones for "educational purposes."[97] The following year, the head of the Ministry of Education reiterated the need to comply with this ban.[98] The specific emphasis on banning personal mobile devices reveals an official intent to compel children to use exclusively school-provided equipment.
3. The coordinated efforts of Rospotrebnadzor and the Ministry of Education notably coincided with the completion of Rostelecom's project to connect schools to the ESPD and the mandatory installation of state-issued root certificates, which enabled traffic monitoring.
4. Official declarations about the harmful effects of screen time seem hypocritical, considering the administrative pressure on children to spend increasing amounts of time online. Many students are required to complete homework and to communicate through

[95] Federal Law of the Russian Federation dated December 19, 2023 No. 618-FZ «О внесении изменений в Федеральный закон "Об образовании..." (On amending the Federal Law "On Education...) https://www.consultant.ru/document/cons_doc_LAW_464808/ (Accessed: 17.08.2026).
[96] See, e.g., Lukyanova, Irina. «Закон о хорошем поведении. Как и зачем депутаты опять отнимают у школьников телефоны» [The law on good behavior. How and why deputies are taking phones away from school children again]. *Novaya Gazeta*, November 7, 2023.
[97] See Paragraph 3.5.3 of the Resolution of the Chief State Sanitary Doctor of the Russian Federation, dated September 28, 2020, No. 28, «Об утверждении санитарных правил СП 2.4.3648-20 "Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи"» (On Approval of Sanitary Rules SP 2.4.3648-20 Sanitary and Epidemiological Requirements for Organizations of Training and Education, Leisure and Health Improvement of Children and Youth) https://www.consultant.ru/document/cons_doc_LAW_371594/a87d3709aa01857b67d2d04477b1d8458572e62e/ (Accessed: 17.08.2026).
[98] Azattyq Asia. «В России запретили использовать телефоны на уроках в школе» [In Russia, the use of phones during school lessons has been banned]. *Radio Free Europe/Radio Liberty*, August 31, 2022. https://www.azattyqasia.org/a/32012530.html (Accessed: 19.08.2026).

the FGIS “My School,” while “educational” platforms continuously expand to include non-educational features such as propaganda feeds, blogs, messaging applications, chatbots, and games.

5. In early 2026, reports surfaced about government plans to completely ban mobile phones for children under a certain age.[99] Notably, this initiative is once again being promoted by Sergey Kravtsov, the head of the Ministry of Education. He did not disclose specific details, instead appearing to “test the waters” for further restrictions on rights and freedoms. Simultaneously, other officials were actively developing kids’ SIM cards and accelerating the expansion of online learning.

Ultimately, all of this demonstrates that the Russian authorities are deliberately driving minors not only onto “approved” online platforms but also onto state-controlled physical devices. These computers and gadgets are not merely fully exposed to surveillance; they also serve as data providers for predictive analytics and the training of state-run AI models.

[99] Efremov, Gennady. «Некоторым россиянам хотят полностью запретить пользоваться сотовыми телефонами и смартфонами. Кого коснется» [Some Russians may face a complete ban on using cell phones and smartphones. Who will be affected]. *CNews,* March 25, 2026.

Perimeter 4.

Monitoring Out-of-School Online Activity

Before officials completely isolate the Russian segment of the internet from the global network and impose a total ban on the use of non-state devices across the entire population, certain online activities by minors still manage to evade surveillance. Controlling children's behavior outside educational institutions and official online platforms is no easy task for the Russian authorities, a fact that clearly causes them deep concern. Moreover, even if kids' SIM cards become standard practice, it will be quite difficult for state agencies to track how minors use adults' smartphones. To bring this elusive sector under control, the authorities have been implementing alternative surveillance practices for years, actively enlisting schools in the process. Three key mechanisms stand out: monitoring by school administrators and faculty; "cyber squads" (Russ. kiberdruzhiny, or "кибердружины," also referred to in English literature as "cyber patrols"); and the neural network systems of federal agencies.

School Social Media Surveillance

In the second half of the 2010s—largely due to the rise of opposition sentiments among teenagers and young adults[100]—school principals, following directives from regional administrations, began informally requiring homeroom teachers to track down students' accounts and to record their online activities.[101] This practice can be described as "administrative cyberstalking," understood here as the informal, institutional tracking of minors' digital footprints that amounts to a gross invasion of their privacy.

As is often the case, the authorities justify these measures by claiming they are necessary to protect children from suicide, drugs, and violence. However, the insincerity of this appeal is evident. Turning teachers into informants destroys any remaining trust and risks driving troubled adolescents even further into isolation. If the Russian authorities were genuinely interested in providing psychological support to minors in distress, they would not create an atmosphere of omnipresent mistrust, instill a culture of sycophancy and denunciation, promote militarism, or use teachers as spies. At the same time, current regulations demonstrate that teacher-led

[100] See, e.g., HRW. «Россия: Школьников и студентов преследуют после протестов» [Russia: Schoolchildren and students targeted after protests]. *Human Rights Watch*, June 23, 2017. https://www.hrw.org/ru/news/2017/06/23/russia-children-students-targeted-after-protests (Accessed: 17.08.2026).
[101] Litoy, Aleksandr. «"Большой брат" от звонка до звонка. Как следят за соцсетями школьников» ["Big Brother" from bell to bell. How school children's social networks are monitored]. *Radio Free Europe/Radio Liberty*, December 22, 2019. https://www.svoboda.org/a/30338558.html (Accessed: 17.08.2026).

monitoring is primarily aimed not at psychological support and rehabilitation but at pervasive surveillance and transferring data to the MVD, with a reliance on disciplinary and repressive measures. Undoubtedly, effectively preventing destructive behavior and supporting children in difficult life situations is the duty of parents, relatives, teachers, and, indeed, all adults. However, the actions of the Russian authorities show that tragedies involving minors are typically exploited as a pretext for introducing ever stricter oversight, which worsens, rather than improves, the mental health of schoolchildren.

By the early 2020s, this administrative cyberstalking had intensified and evolved into the surveillance of—and crackdown on—virtually any critique of the Russian regime and its policies by students.[102] Concurrently, the authorities began gradually legalizing these practices among school staff and, as a result, local regulations mandating the "monitoring of social networks" started to appear at the levels of individual educational institutions, municipalities, and regions.[103] These regulations—many of which remain in effect—typically contain algorithms and methodological recommendations instructing homeroom teachers to conduct regular audits of their students' accounts and record in special logs the minors' social circles, their online community interests, and even their comments and likes. For example, a directive issued in the Saratov region stipulates that if a teacher discovers certain information on a student's page—ranging from the use of "*drug-related slang*" or expressions of "*anger*" to membership in groups that "*incite unlawful acts*" or vague catch-all terms like "*and so forth*"—they are required to report it to the school principal,[104] who is then instructed to cooperate with the MVD.[105] The

[102] See, e.g., Savitskaya, Lyudmila. «Срочно удали лайк, иначе утром подают в полицию» [Delete the like immediately, otherwise they will file a report with the police in the morning]. *Radio Free Europe/Radio Liberty,* January 28, 2021. https://www.svoboda.org/a/31074785.html (Accessed: 26.05.2026); Lugovskaya, Elizaveta. «За вашими детьми следят. Кто и зачем просит учителей мониторить соцсети учеников» [Your children are being watched. Who asks teachers to monitor students' social networks and why]. *Mel*, April 28, 2021.

[103] Education authorities and schools across various Russian regions began actively publishing orders to monitor social media in 2021. Here are just a few typical examples: Order of the Committee of Education and Science of the Kursk Region, dated May 20, 2021, No. 1-552, «Об организации в образовательных организациях Курской области мониторинга аккаунтов обучающихся в социальных сетях» (On the Organization of Monitoring of Students' Accounts in Social Networks in Educational Organizations of the Kursk Region); Order of the Education Department of the Administration of the Ivanteevka Municipal District of the Saratov Region, dated November 10, 2022, No. 211, «О проведении мониторинга социальных сетей несовершеннолетних» (On Conducting Monitoring of Minor's Social Networks) https://uoivanteevka.ucoz.ru/sport/prikaz_o_prov_mon_socset_22.pdf (Accessed: 19.08.2026); Order of the Education Department of the Tavda Urban Okrug of the Sverdlovsk Region, dated February 19, 2024, No. 109, «Об утверждении Порядка проведения мониторинга аккаунтов социальных сетей несовершеннолетних в образовательных организациях в новой редакции» (On Approval of the Procedure for Monitoring Social Network Accounts of Minors in Educational Organizations in the New Edition); Order of the MBOU "Lyceum No. 1" of Dobrinka Settlement, Lipetsk Region, dated September 1, 2025, No. 386, «Приказ о мониторинге социальных сетей обучающихся» (On Monitoring of Students' Social Networks) https://lic1dobrinka.gosuslugi.ru/netcat_files/196/2998/Prikaz_o_monitoringe_sotsial_nyh_stey_obuchayuschihsya.pdf (Accessed: 19.08.2026).

[104] See, e.g., Order of the Education Department of the Administration of the Ivanteevka Municipal District of the Saratov Region, dated November 10, 2022, No. 211, «О проведении мониторинга социальных сетей несовершеннолетних» (On Conducting Monitoring of Minor's Social Networks) https://uoivanteevka.ucoz.ru/sport/prikaz_o_prov_mon_socset_22.pdf (Accessed: 19.08.2026).

[105] Ibid.

materials also offer practical advice to teachers, effectively training them in methods of undercover infiltration by advising them, for instance, "*not to impose themselves or their views on teenagers... to observe... and to be natural and sincere*" in order to gain the minors' trust and access their private pages.[106]

In recent years, this social media monitoring by educators has not only been gradually codified but has also been integrated with centralized algorithms and evaluation criteria. For example, in early 2025, the Federal Agency for Youth Affairs (Rosmolodezh) sent a letter to regional authorities requesting the dissemination—among subordinate organizations, including educational institutions—of "*methodological guidelines and informational materials on preventing the spread of terrorism, extremism, and neo-Nazism, taking into account modern challenges and threats.*"[107] Although the letter's subject line emphasizes "preventive work" among youth from Ukrainian territories occupied by the Russian authorities, its scope is much broader, and the stated focus merely serves as a pretext for implementing blanket surveillance. These methodological materials provide schools and other state and municipal bodies with recommendations covering various aspects of control, including indoctrination, standardization, and the system of rewards and punishments.[108]

A significant portion of Rosmolodezh's recommendations focuses on organizing surveillance—both through direct observation and social media monitoring—with Section 7 dedicated to the latter, instructing school staff to track status updates, subscriptions, post content, images, videos, and music. Rosmolodezh's authors identify six *"risk groups subscribing to terrorist or extremist ideologies, including neo-Nazism and radical nationalism, whose members can be identified by analyzing their social media accounts*."[109] When citing examples of markers indicating affiliation with these "risk groups," the authors highlight posts and comments that "*convey the views of 'foreign agents'*" («иностранный агент», or "foreign agent" is a label typically used to target and criminalize political dissent), any publications expressing "*opposition or anti-Russian sentiments*,"[110] subscriptions to "*pro-Ukrainian communities*," and any criticism of the war launched by the Russian authorities against Ukraine.[111] In other words, Rosmolodezh staff employ a common manipulative tactic to define these "risk groups": on the one hand, they conflate concepts to equate entirely legitimate civic, human rights, or pacifist stances with neo-Nazi chauvinistic ideology; on the other, they introduce distorted and vague criteria for "extremism" to enable the labeling of anyone whose views diverge from the Russian regime's

[106] Ibid.
[107] Letter of the Federal Agency for Youth Affairs, dated February 27, 2025, No. GG/1449-06, «О направлении методических рекомендаций» (On Sending Methodological Recommendations) https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=871483 (Accessed: 11.09.2026).
[108] Federal Agency for Youth Affairs. Guidelines on preventing the spread of the ideology of terrorism, extremism and neo-nazism approved by the letter of Rosmolodezh dated February 27, 2025 No. GG/1449-06.
[109] Ibid. P. 37.
[110] Ibid. P. 38–40.
[111] Ibid.

chauvinistic ideology as a dangerous radical. Regarding the organization of this surveillance, the materials note that monitoring "*must be conducted on an ongoing basis within educational institutions, and preventive work must be adjusted based on the findings*."[112] Finally, the materials make it abundantly clear that this "preventive work" is effectively under the control of law enforcement and security agencies.[113]

Judging by the seven-step procedure outlined in that same Section 7 of the Rosmolodezh text, students' "social passports"—which school staff are mandated to compile and systematically maintain (see above)—play a central role in recording online monitoring results.[114] This indicates that the Russian regime is integrating "social passports"—originally introduced in the late 1990s as tools for social, humanitarian, and educational support in schools—into an infrastructure of total surveillance. Under this framework, the authorities are supplementing existing data on a family's social status, composition, living conditions, and financial well-being, as well as a child's psychological or physiological characteristics, with information gathered through social media monitoring. Furthermore, each student's "social passport" is technologically linked to (1) the "social passport of the class"; (2) the minor's digital profile in the FGIS "My School"; and (3) the case file in the State Information System "Prevention" (see below), if such a record has been created for the child.

Alongside the dissemination of its infamous guidelines,[115] Rosmolodezh is taking further steps to centralize social media surveillance, moving beyond the individual monitoring conducted by school staff. For example, in early 2026, it emerged that Tatarstan authorities, exerting pressure through schools, had begun demanding that parents provide details about all their children's online accounts—including messengers and social networks—as well as their phone numbers. The declared rationale was that this data collection aimed to facilitate "*interagency cooperation with the State Budgetary Institution 'Republican Center for Youth, Innovation, and Prevention Programs: Navigator.*'"[116] Crucially, while this center was legally established by the Ministry of Youth Affairs of the Republic of Tatarstan, it is simultaneously integrated into the nationwide agenda and project framework of Rosmolodezh. Almost concurrently—and likely as part of the same overarching federal campaign—Tatyana Savinova, Deputy Governor of the Sverdlovsk

[112] Ibid. P. 35.
[113] Ibid. P. 10, 22, 23, 25, 35–36.
[114] Ibid. P. 36.
[115] Amnesty International examined certain aspects of the "Methodological Recommendations on Preventing the Spread of the Ideology of Terrorism, Extremism, and Neo-Nazism" issued by Rosmolodezh, as well as the agency's methodological materials concerning traditional monitoring, see pages 16–19 here: Amnesty International. *"Only official sources" : Indoctrination in the Russian educational system*. Amnesty International, June 1, 2026. https://www.amnesty.org/en/wp-content/uploads/2026/06/EUR4609562026ENGLISH.pdf (Accessed: 15.09.2026).
[116] RFE/RL. «"Насилие не остановить ни мониторингом, ни запретом соцсетей". О попытках властей усилить контроль за школьниками в интернете» ["Violence cannot be stopped by monitoring or banning social networks." On the authorities' attempts to tighten control over school children online]. *Radio Free Europe/Radio Liberty*, February 17, 2026. https://www.svoboda.org/a/nasilie-ne-ostanovit-ni-monitoringom-ni-zapretom-sotssetey-o-popytkah-vlastey-usilit-kontrol-za-shkolnikami-v-internete/33680397.html (Accessed: 27.05.2026).

Region, announced the launch of an automated monitoring system covering 4.6 million accounts belonging to minors.[117] Neither the technical details nor the specific parameters of this system have been clarified. It also remains unclear exactly whose accounts are being targeted, given that statistics place the adolescent population of the Sverdlovsk Region at approximately 150,000 to 200,000. Since this is a federal project, it is highly probable that many other regions are already implementing similar measures without publicly announcing them. At the same time, it is evident that some constituent entities of the Russian Federation—due to underdeveloped infrastructure—continue to rely on manual monitoring carried out by teachers, as demonstrated, for example, by the approach taken in the Belgorod Region.[118]

When assessing the new practices announced by the authorities of Tatarstan and the Sverdlovsk Region, even independent media outlets[119] overlook key features: first, monitoring children's internet activity has evolved into a coordinated effort comprising schools, regional administrations, local branches of Rosmolodezh, the FSB, and the MVD; second, it enlists parents as unwitting accomplices in establishing total surveillance; third, it extends beyond social media to encompass a minor's entire accessible digital footprint and phone metadata; and fourth, it increasingly relies on AI-driven tools. Under this new scheme, school staff act as grassroots data collectors, tasked with obtaining students' mobile phone numbers and their social media and messaging account details from parents. However, the primary analytical work behind this tracking is handled by federal and regional agencies. If content classified by the authorities as "destructive" is detected, an orchestrated mechanism of administrative pressure is triggered, involving not only teachers, social workers, and school administrators but also external bodies such as regional Commissions on Juvenile Affairs and the Protection of Their Rights (КДН и ЗП, or KDN i ZP), MVD's Juvenile Delinquency Units (ПДН, or PDN), and child protective services.

Nevertheless, this does not mean that the authorities intend to exempt all teachers from direct internet oversight. The extent of teacher involvement in this process seems to depend on regional officials. By all indications, the administrations of certain federal subjects plan to continue these

[117] Novaya Gazeta Europe. «Свердловские власти начали мониторить соцсети школьников на предмет "запрещенного" контента» [Sverdlovsk authorities have begun monitoring school children's social networks for "banned" content]. *Novaya Gazeta Europe*, March 11, 2026. https://novayagazeta.eu/articles/2026/03/11/sverdlovskie-vlasti-nachali-monitorit-sotsseti-shkolnikov-na-predmet-zapreshchennogo-kontenta-news (Accessed: 19.08.2026).

[118] Mel. «Губернатору Белгородской области пожаловались, что учителей заставляют мониторить соцсети школьников и заполнять по ним отчеты» [The Governor of the Belgorod Region was complained to that teachers are forced to monitor school children's social networks and fill out reports on them]. *Mel*, March 22, 2026.

[119] RFE/RL. «"Насилие не остановить ни мониторингом, ни запретом соцсетей". О попытках властей усилить контроль за школьниками в интернете» ["Violence cannot be stopped by monitoring or banning social networks." On the authorities' attempts to tighten control over school children online]. *Radio Free Europe/Radio Liberty*, February 17, 2026. https://www.svoboda.org/a/nasilie-ne-ostanovit-ni-monitoringom-ni-zapretom-sotssetey-o-popytkah-vlastey-usilit-kontrol-za-shkolnikami-v-internete/33680397.html (Accessed: 27.05.2026).

activities, sometimes in their previous form and sometimes under the guise of school-based "cyber squads."

Cyber Squads

Even before the advent of administrative cyberstalking and widespread internet surveillance through AI-driven algorithms, certain quasi-public structures began paying special attention to the online behavior of minors—particularly on social media platforms. Prominent among them was the para-state Safe Internet League (Лига безопасного интернета), established by Kremlin-aligned business entities in close coordination with the MVD, Mintsifry, and the State Duma Committee on Family, Women, and Children. The Safe Internet League's initial activities included monitoring children's digital conduct, collaborating with schools, and organizing cyber squads tasked with notifying law enforcement agencies—primarily the MVD—about the online posting of content designated by officials as "prohibited" or "destructive."[120] Under this pretext, alongside child sexual abuse material, drug trafficking, and the promotion of suicide, they tracked criticism of the authorities, participation in opposition movements, and the planning of peaceful protests.[121]

For a long time, the activities of the Safe Internet League and its cyber squads[122] were masked as grassroots civic initiatives, though since the second half of the 2010s, many federal subjects, municipalities, and schools have openly cooperated with these structures,[123] with some even issuing regulations governing this "interaction."[124] And in fact, this went far beyond mere interaction. Indeed, documents from certain regional executive bodies reveal that as early as the second half of the 2010s, Russian officials had begun using schools as bases for creating and deploying cyber squads. For example, Resolution No. 11, issued on March 17, 2022, by the Nefteyugansk Municipal Commission on Juvenile Affairs and the Protection of Their Rights,

[120] See, e.g., Daucé, Françoise, Benjamin Loveluck, Bella Ostromooukhova, and Anna Zaytseva. "From Citizen Investigators to Cyber Patrols: Volunteer Internet Regulation in Russia". *Laboratorium: Russian Review of Social Research* 11 (3) (2020): 46–70.
[121] Ibid.
[122] The Safe Internet League set the precedent for creating "cyber squads"; following its lead, other—predominantly pro-Kremlin—groups began establishing similar units, effectively acting as online combat squads. For instance, so-called "Cossack organizations" were particularly active in this regard (Daucé, Françoise, Benjamin Loveluck, Bella Ostromooukhova, and Anna Zaytseva. "From Citizen Investigators to Cyber Patrols: Volunteer Internet Regulation in Russia". *Laboratorium: Russian Review of Social Research* 11 (3) (2020): 46–70).
[123] Roskomsvoboda. «Регионы заводят себе кибердружины» [Regions are establishing cyber squads]. *Roskomsvoboda*, October 9, 2019. https://roskomsvoboda.org/ru/50250/ (Accessed: 27.08.2026).
[124] See, e.g., Resolution of the Government of the Belgorod Region, dated May 22, 2017, No. 181-pp, «Об организации деятельности кибердружин Белгородской области» (On the Organization of Activities of Cyber Squads of the Belgorod Region); Resolution of the Government of the Republic of Buryatia, dated July 12, 2019, No. 378, «Об утверждении Порядка взаимодействия с кибердружинами в Республике Бурятия» (On Approval of the Procedure for Interaction with Cyber Squads in the Republic of Buryatia); Resolution of the Government of the Novgorod Region, dated September 23, 2024, No. 457, «Об утверждении Регламента деятельности кибердружин в Новгородской области» (On Approval of the Regulations on the Activities of Cyber Squads in the Novgorod Region).

explicitly references orders from the local Department of Education dating back to 2017–2018. These orders mandated the appointment of municipal coordinators and the establishment of cyber squads directly "*within general education organizations*."[125] This process reportedly intensified in 2022–2023, although the extent and mode of school involvement varied significantly by region. In some federal subjects, school principals issued direct orders to set up cyber squads composed of both staff members and high school students.[126] Other regions facilitated the recruitment of minors into cyber squads by external entities, such as Russian Cossack associations or organizations affiliated with Rosmolodezh.

However, it was not until 2026 that the Russian Government formally incorporated cyber squads into federal legislation through Directive No. 1030-r, dated April 30, 2026. This directive outlined the following state measure: "*Organizing activities to prevent negative social phenomena among students within educational institutions, including the establishment and/or activation of cyber squads—engaging active students from vocational educational institutions—and media patrols*."[127] By doing so, the authorities not only officially codified the activities of cyber squads at the federal level but also openly redefined these quasi-civic groups as state-run entities. Notably, the directive does not explicitly mention schoolchildren, and officials maintain that participation in such groups is voluntary. However, as is often the case, the reality differs: the squads are formed through the active recruitment of schoolchildren, and all evidence suggests that these are not spontaneous initiatives but rather planned, top-down activities implemented through the intensive use of administrative pressure.

Neural Network Systems of Federal Agencies

[125] Resolution of the Municipal Commission on Juvenile Affairs and Protection of Their Rights in the City of Nefteyugansk dated March 17, 2022 No. 11 «Об обеспечении информационной безопасности несовершеннолетних...» (On ensuring the information security of minors...) https://www.admugansk.ru/uploads/2023/02/%E2%84%96_11_ot_17.03.2022.doc (Accessed: 16.09.2026).
[126] See, e.g., Directive of the School Principal of the State Budgetary Educational Institution "Basic General Education School No. 21 of the City of Novokuybyshevsk, Samara Region" dated August 19, 2022 No. 104-OD «Об утверждении кибердружины...» (On the approval of the cyber squad...) http://nov21ooh.minobr63.ru/wp-content/uploads/2023/11/приказ-об-утверждении-кибердружины-буллинг.pdf (Accessed: 18.08.2026); Order of the MOBU "Secondary General Education School No. 23", dated September 1, 2023, No. 458, «О создании и деятельности кибердружины МОБУ СОШ № 23 в 2023-2024 учебном году» (On the Creation and Activities of a Cyber Squad of MOBU SOSh No. 23 in the 2023-2024 Academic Year) https://taganschool23.ru/2023-2024/Kiberdrujina/prikaz_o_sozdanii_kiberdruzhiny.pdf (Accessed: 17.08.2026); Directive of the School Principal of the Municipal Educational Institution "Secondary School No. 25 of the Kirovsky District of Volgograd" dated April 23, 2025 No. 75 «О создании и функционировании Кибердружины» (On the creation and functioning of the Cyber squad) https://sosh25-vlg2012.ucoz.ru/food2/prikaz_o_sozdanii_kiberdruzhiny.pdf (Accessed: 18.08.2026).
[127] Directive of the Government of the Russian Federation dated April 30, 2026 No. 1030-r «Об утверждении комплекса мер...» (On approval of a set of measures...) https://www.consultant.ru/document/cons_doc_LAW_533626/ (Accessed: 17.08.2026).

For years, numerous state agencies—most notably the MVD, Roskomnadzor, Rosmolodezh, the Presidential Administration, the Federal Guard Service, and the FSB—have conducted extensive, large-scale internet surveillance.[128]

Since the mid-2010s, AI-driven online monitoring systems have played an increasingly significant role. For instance, the MVD actively employs programs such as "FindFace," "Insider" (Инсайдер), "Cribrum" (Крибрум), "SEUS" (СЕУС), "Seriya," "Klon" (Клон), and "Konyunktura" (Конъюнктура).[129] Roskomnadzor, primarily through its Main Radio Frequency Center (ГРЧЦ, or GRChTs), utilizes various software suites, including Oculus (Окулус), Vepr (Вепрь), and Chisty Internet (Чистый интернет).[130] While the list of state agencies and monitoring tools could be extended further, the sheer scale of these operations is already evident. Neural networks are now capable of identifying students even from low-quality photographs, detecting protest or opposition imagery, deciphering hidden meanings in slang, and using various indicators to flag links to organizations designated by officials as "undesirable."

The systems mentioned above do not specifically target children. However, when it comes to the surveillance of minors in particular, the primary federal agency coordinating this activity—as is clear from the preceding context—is Rosmolodezh. In turn, a key role in online monitoring within this state body is played by the so-called "Center for Studying and Network Monitoring of the Youth Environment" (ЦИСМ, or CISM). It utilizes neural networks to monitor millions of social media accounts belonging to teenagers and young adults in real time, scanning for "destructive content." To capture and organize this data, CISM developed the Automated Information System "Prevention" (Автоматическая информационная система «Профилактика»), which was also equipped with a variety of other functions. In 2025, it was revealed that this software had been transferred to the Ministry of Education, which announced a tender to modernize and scale it up to the federal level.[131] Simultaneously, the platform was renamed the State Information System "Prevention" (Государственная информационная

[128] For a very brief overview of the Russian state surveillance system see, e.g., Dossier Center. «Глаза Кремля. Как устроен цифровой ГУЛАГ в России — и что мешает ему заработать в полную силу» [The Eyes of the Kremlin. How the digital GULAG is structured in Russia — and what prevents it from operating at full capacity]. *Dossier Center,* March 11, 2024. https://dossier.center/sorm/ (Accessed: 15.05.2026).
[129] See, e.g., Meduza. «Полиция по всей России покупает системы мониторинга соцсетей. Они помогают искать экстремизм "не выходя из рабочего кабинета"» [Police across Russia buy social media monitoring systems. They help search for extremism "without leaving the office"]. *Meduza*, October 16, 2018. https://meduza.io/feature/2018/10/16/politsiya-po-vsey-rossii-pokupaet-sistemy-monitoringa-sotssetey-oni-pomogayut-iskat-ekstremizm-ne-vyhodya-iz-rabochego-kabineta (Accessed: 15.05.2026).
[130] See, e.g., Agents. «Крупнейший взлом российской цензуры: как она охраняет здоровье Путина, помогает Навке, заводит досье на журналистов и разводит ботов» [The biggest hack of Russian censorship: how it protects Putin's health, helps Navka, creates dossiers on journalists, and spawns bots]. *Agents*, February 8, 2023. https://www.agents.media/tsenzura/ (Accessed: 27.04.2026).
[131] Maleva, Yuliya and Tatyana Akinshina. «Минпросвещения разработает ГИС для профилактики детской преступности» [The Ministry of Education will develop a GIS for the prevention of juvenile delinquency]. *Vedomosti*, September 4, 2025.

система «Профилактика»), and its official launch took place on December 1 of that same year.[132]

The GIS "Prevention" offers extensive functionality and was designed by CISM to serve as a unified record-keeping database. It consolidates details on neglected and at-risk adolescents, offenses committed by minors, and dysfunctional families, with the aim of standardizing, analyzing, and distributing this data. Under Russian Government Resolution No. 411, dated April 1, 2025, numerous agencies contribute to the system by sharing a wide range of information. This includes the personal data of children and their legal representatives, as well as records concerning minors running away from home, drug use, child abuse, and offenses committed. The system also accumulates data on minors' placements in shelters, rehabilitation centers, or prevention facilities; the termination of parental rights; corrective measures; social assistance provided; and much more. Furthermore, the GIS "Prevention" is integrated into the broader state information architecture.[133] This means that via the Unified System of Identification and Authentication (ESIA), the GIS "Prevention" links its case files with children's digital profiles (both student profiles within the FGIS "My School" and general profiles).

Although Resolution No. 411 does not explicitly disclose this, there is little doubt that the case files of minors within the GIS "Prevention" incorporate data obtained through online surveillance—whether through the administrative cyberstalking performed by homeroom teachers, the activities of cyber squads, or monitoring by federal agencies. This information is likely categorized in the founding document of the GIS "Prevention" under vague headings such as "*offenses*" and "*anti-social acts*," or placed under the bureaucratic phrase: "*circumstances enabling the Commission on Juvenile Affairs and the Protection of Their Rights to consider conducting individualized preventive work with the minor.*"[134] Under this latter category, officials apparently include any legal or factual grounds (such as school alerts, cyber squad reports, or findings from automated monitoring systems) that local authorities deem sufficient to initiate an investigation into a child, including likes, reposts, and browsing history on the websites of organizations designated by the Russian state as "undesirable."

It is clear that the rollout of the GIS "Prevention," alongside improving the efficiency of Rosmolodezh's monitoring, was precisely what the previously mentioned administrative measures by the authorities of Tatarstan and the Sverdlovsk region were intended to serve. This indicates that the processes described are not isolated initiatives, despite attempts by propaganda media and officials to downplay or deny the involvement of schools in surveillance. The nationwide scope of this project is further evidenced by the very same Russian Government

[132] Resolution of the Government of the Russian Federation dated April 1, 2025 No. 411 «О государственной информационной системе профилактики...» (On the state information system for prevention...) https://www.consultant.ru/document/cons_doc_LAW_502345/ (Accessed: 20.08.2026).
[133] Ibid.
[134] Ibid.

Directive No. 1030-r, since this document not only institutionalizes the activities of cyber squads but also calls for intensifying surveillance, control, and propaganda among minors and young adults. Several measures outlined in the document seek to improve coordination between regional administrations and other bodies, including the MVD and Rosgvardiya. Measure No. 38 specifically addresses internet tracking; it designates the "*constituent entities of the Russian Federation*" as the locations for implementation and identifies Rosmolodezh as the executing agency—the very agency for which schools in Tatarstan are collecting student account data.[135] All of this demonstrates that the expansion of Rosmolodezh's monitoring, the administrative pressure exerted in schools to force parents to hand over their children's account data, and the modernization of the GIS "Prevention" are components of a single project aimed at centralizing and strengthening the Russian state surveillance machine.

As of the early autumn of 2026, there are no clear indications that a fully operational predictive analytics engine for children's behavior exists within the GIS "Prevention." However, the system's architecture and functionalities suggest that the authorities are moving decisively in that direction, and certain modules may have already undergone testing. Even now, the GIS "Prevention" is not merely a database for recording, storing, and sharing information about children deemed by the authorities to require special attention. It also serves as a digital organizer with assessment capabilities: it signals officials and staff of the relevant agencies regarding the need for specific preventive actions (such as conducting a preventive talk or launching a rehabilitation program), evaluates the effectiveness of the work performed, recommends assigning a particular legal status to a child, and assists in drafting individualized plans for various scenarios. While the system currently operates as a sophisticated yet conventional automated platform, there is little doubt that the authorities' ultimate goal is to deploy predictive analytics—including child-ranking algorithms—covering both those with existing case files in the GIS "Prevention" and, more broadly, those with digital profiles.

All of this demonstrates that state monitoring of minors' online activities has reached a qualitatively new level, transforming it into a single mechanism that is, in turn, integrated into the architecture of total control. At the top of this vertical structure are the federal authorities (the MVD, the FSB, Roskomnadzor, Rosmolodezh, and Rosgvardiya), which conduct surveillance themselves while simultaneously receiving reports and denunciations from subordinate bodies. Below them are para-state censorship organizations, such as the Safe Internet League, operating at a nationwide level. Further down are the regional administrations and their departments responsible for "working with" minors and young adults. At the grassroots level, university and college students, social workers, principals, teachers, and schoolchildren themselves participate in the surveillance.

[135] Directive of the Government of the Russian Federation dated April 30, 2026 No. 1030-r «Об утверждении комплекса мер...» (On approval of a set of measures...) https://www.consultant.ru/document/cons_doc_LAW_533626/ (Accessed: 17.08.2026).

Auxiliary Perimeters under Construction

Targeted state surveillance of minors is not limited to the perimeters listed above. The Russian authorities are implementing additional measures and devising new methods. Although it is impossible to cover all of them in a brief overview, several key initiatives merit mention.

Kids' SIM Cards and Control of Mobile Communications

Since mid-2025, officials have been actively developing—and, in the summer of 2026, officially began rolling out—so-called "kids' SIM cards." This innovation is part of a broader strategy to strictly link persons to their mobile devices and subscriber numbers. In recent years, the authorities have taken several major steps toward executing this agenda, including:

- Limiting the number of SIM cards that can be registered to a single user.[136]
- Tethering SIM cards and phones to each other, as well as to their owners, who are prohibited—with rare exceptions—from transferring them to third parties.[137]
- Introducing additional data verification requirements for all mobile service contracts, including video recording of the contract-signing process at points of sale (a requirement that came into effect on September 1, 2025).[138]
- Compelling mobile operators to immediately block any attempts to use a subscriber number on a different device.[139]
- Creating a unified IMEI database by the spring of 2027—essentially a registry tracking which citizens own specific mobile devices.[140]

As this agenda took shape in the summer and autumn of 2025, Mintsifry—under the guise of protecting minors from scammers and dangerous websites—announced the development of kids' SIM cards,[141] even though Russian mobile operators were already offering various plans with parental controls. Even Dmitry Grigorenko, Chief of Staff of the Russian Government

[136] See Article 1 of the Federal Law of the Russian Federation dated August 8, 2024 No. 303-FZ «О внесении изменений в Федеральный закон "О связи"...» (On amending the Federal Law "On Communications"...) https://www.consultant.ru/document/cons_doc_LAW_482565/ (Accessed: 28.08.2026).
[137] See Article 9 of the Federal Law of the Russian Federation dated April 1, 2025 No. 41-FZ «О создании государственной информационной системы противодействия правонарушениям...» (On the creation of the state information system for countering offenses...) https://www.consultant.ru/document/cons_doc_LAW_502182/ (Accessed: 28.08.2026).
[138] Resolution of the Government of the Russian Federation dated December 30, 2024 No. 1994 «Об утверждении Правил оказания услуг телефонной связи...» (On approval of the Rules for the provision of telephone communication services...) https://www.consultant.ru/document/cons_doc_LAW_495347/ (Accessed: 20.08.2026).
[139] Federal Law of the Russian Federation dated June 26, 2026 No. 210-FZ «О внесении изменений в Федеральный закон "О связи"...» (On amending the Federal Law "On Communications"...) https://www.consultant.ru/document/cons_doc_LAW_537891/ (Accessed: 03.08.2026).
[140] Ibid.
[141] Lyubavina, Anna. «Школьников предлагают пересадить на специальные SIM-карты» [It is proposed to transfer school children to special SIM cards]. *CNews*, September 25, 2025.

Apparatus, acknowledged this, adding that officials wanted to "*formalize this practice and make it systematic*."[142] As the initiative unfolded, the authorities once again leveraged rhetoric about protecting children's interests with the true aim of strengthening and centralizing total surveillance—thereby violating the very rights they claim to defend.

At the regulatory level, the kids' SIM cards initiative was introduced through the same federal law that mandated the creation of a unified IMEI database, with both provisions scheduled to take effect on March 1, 2027.[143] Under this legislation, the authorities granted parents the "right" to notify their mobile operator that a particular number is being used by a minor. Upon receiving this notification, the operator is required to enter the line into the relevant register and activate the corresponding restrictions for that account. The law itself does not specify the rules for these SIM cards, stating only that they are to be established by the Russian Government.[144]

Notably, the authorities initially planned to mandate that parents register their children's phone numbers, threatening sanctions for non-compliance. However, officials shortly afterward announced that the scheme would be "voluntary"—a shift likely driven by the extreme complexity of implementing such a framework. This step back, however, should not mislead anyone. The Russian authorities rarely abandon repressive measures and in their bureaucratic parlance, "voluntary participation" usually implies the exertion of covert institutional pressure. In cases of child surveillance, as demonstrated by many of the examples cited above, schools are almost always the vehicle for this coercion. Statements by officials confirm that events are unfolding according to this very pattern. For instance, at the outset of the discussion regarding kids' SIM cards, Sergey Rybalchenko, Chairman of the Commission on Demography, Protection of Families, Children, and Traditional Family Values of the Civic Chamber of the Russian Federation, stated that the authorities plan to provide children with access to school networks and digital services specifically through these cards.[145] Consequently, there is a high probability that officials intend to deny access to free internet in educational institutions—and possibly even to the FGIS "My School"—to those children whose parents have not registered such numbers. In other words, the temporary easing of requirements has been introduced solely to prepare the necessary infrastructure and establish regulations; in the Russian context, the actual operation of such systems almost never aligns with the proclaimed "voluntary" nature.

As far as is currently known, under the authorities' plan, when mobile operators learn that a subscriber number is used by a child, they are mandated to record this information in their

[142] Shvetsova, Anna. «Цифровой щит для ребенка. Что скрывается за идеей специальных детских SIM-карт» [Digital shield for a child. What lies behind the idea of special kids' SIM cards]. *ComNews,* April 13, 2026.
[143] See Article 11 of the Federal Law of the Russian Federation dated June 26, 2026 No. 210-FZ «О внесении изменений в Федеральный закон "О связи"...» (On amending the Federal Law "On Communications"...) https://www.consultant.ru/document/cons_doc_LAW_537891/ (Accessed: 03.08.2026).
[144] See Article 1, ibid.
[145] Lyubavina, Anna. «Школьников предлагают пересадить на специальные SIM-карты» [It is proposed to transfer school children to special SIM cards]. *CNews*, September 25, 2025.

databases and report it to Roskomnadzor's state monitoring system (ГИС КСИМ, or GIS KSIM). Furthermore, judging by the enacted legislation and measures under preparation, mobile operators will be required to:

- Strictly filter content.
- Offer specialized mobile plans.
- Continuously track physical movements.
- Prohibit roaming.
- Restrict usage exclusively to state-approved social networks and messaging applications (VKontakte, the Sferum platform, and the Max messenger).
- Block calls and messages from foreign numbers, as well as any unauthorized SMS mailings.[146]

In practice, this means that kids' SIM cards will prevent the registration or updating of accounts on independent messaging platforms or any services requiring SMS-based authentication.[147] Although officials deny this scenario, there is a high probability that they plan in the foreseeable future to reduce accessible content to a so-called "whitelist" of websites—similar to the one the Ministry of Education had already established (based on the federal list) for school internet access.[148] As for parents, they will be left with only the ability to change certain minor settings.

Location Tracking

Beyond content filtering and in-depth monitoring of online activity, the authorities openly acknowledge that they plan to use kids' SIM cards to closely track minors' physical movements. While officials frame this once again as a service for parents and a safety measure, its true purpose is to establish mass, systematic state surveillance over children's locations and routes outside of school. To be sure, applications, smartwatches, and standalone devices performing this function for parents have long been available on the market. However, this data remained siloed outside of state-run platforms, creating an obstacle for the totalizing surveillance machine. Consequently, the geotracking technologies tested since 2025 on migrants arriving in Moscow

[146] Draft Resolution of the Government of the Russian Federation, prepared by the Ministry of Digital Development of the Russian Federation, project ID 02/07/07-26/00169086, as of July 6, 2026, «О внесении изменений в постановление Правительства Российской Федерации от 30 декабря 2024 г. N 1994» (On Amending the Resolution of the Government of the Russian Federation of December 30, 2024 No. 1994) https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=PNPA&n=124111 (Accessed: 25.08.2026).
[147] The Insider. «Минцифры предложило запретить детям получать SMS-рассылки. Операторы беспокоятся, что это может перекрыть им доступ к мессенджерам» [Ministry of Digital Development proposed to ban children from receiving SMS blasts. Operators worry this might cut off their access to messengers]. *The Insider*, August 7, 2026. https://theins.ru/news/295794 (Accessed: 25.08.2026).
[148] Official Communication of the Ministry of Education of the Russian Federation, dated November 14, 2025, «О разрешенном перечне интернет-ресурсов для использования в образовательном процессе» (On the Approved List of Internet Resources for Use in the Educational Process) https://www.consultant.ru/document/cons_doc_LAW_518910/ (Accessed: 25.08.2026).

and the Moscow region for long-term, visa-free stays were—as suspected from the very beginning—destined to be scaled to other segments of the population.[149] Clearly, the next major group whose physical movements and routes the Russian regime plans to bring under especially strict control is teenagers.

Moreover, the Russian authorities are taking measures to roll out geotracking across the entire population under their control. To this end, they have mandated that mobile operators start feeding full location data of all their clients into the so-called "data lake" of the Unified State Data Management Platform (ЕИП НСУД, or EIP NSUD) by 2027.[150] However, since a phone number can be purchased by one person and used by another, mass personalized surveillance requires the authorities to know exactly who is using each device. To achieve this, officials have approved the general provisions mentioned above to link mobile devices and phone numbers to designated individuals, while also implementing additional protocols targeting specific large groups of particular interest to the state: migrants and minors.

"Empathetic" Chatbots and "Soul Analytics"

Another large-scale, high-tech approach to establishing total control over minors is the deployment of AI-powered chatbots. When tailored for these purposes, these tools serve as highly effective instruments for indoctrination, predictive analytics, and surveillance. In May 2026, news surfaced that Rosmolodezh was developing a chatbot designed, according to technical specifications, to provide "*sustained, personalized, and empathetic support*"[151] to teenagers and young adults. Unlike existing chatbots on state educational platforms, this service is intended to engage in dialogue across a wide range of topics, focusing on the problems, anxieties, and emotional conditions of schoolchildren and university students—thereby attempting to scan and track their innermost thoughts and feelings.[152]

Rosmolodezh plans to integrate this chatbot into the Max messenger, which, as previously noted, incorporates Sferum—itself part of the FGIS "My School."[153] As also mentioned, registering for Sferum requires authentication via the "Gosuslugi" portal. Consequently, the chatbot will log all conversation details (with whom, when, and about what), linking this data directly to the user's

[149] Troitskiy, Konstantin. *The State Information Resource 'Digital Profile of a Foreign National' and the Shaping of a New Russian Totalitarianism*. Memorial Human Rights Defence Centre, 2026. https://memorialcenter.org/uploads/Konstantin_Troitskiy_The_State_Information_Resource_Digital_Profile_of_a_Foreign_National_and_the_Shaping_of_a_New_Russian_Totalitarianism_7b9d44affa.pdf (Accessed: 15.09.2026).
[150] Lyubavina, Anna. «На развитие российской системы управления данными выделят почти шесть миллиардов» [Almost six billion will be allocated for the development of the Russian data management system]. *CNews*, March 7, 2025.
[151] Maleva, Yuliya. «Молодежь планируют нравственно обогащать через чат-боты» [They plan to morally enrich the youth through chat-bots]. *Vedomosti*, May 12, 2026.
[152] Ibid.
[153] Ibid.

digital profile. If the platform becomes operational, this information will be accessible not only to Rosmolodezh administrators but also to other agencies involved in the project, as well as law enforcement and security services (the MVD, the FSB, the Investigative Committee, and the Prosecutor's Office).

Given that the technical specifications mandate "*centralized storage, along with capabilities for monitoring and controlling the processing of inquiries*," and stipulate that conversations will be analyzed for "*current requests, thematic trends, and behavioral patterns*,"[154] it is clear that the Rosmolodezh chatbot is designed to employ predictive analytics technologies. In other words, the authorities intend to use this data to compile ratings, forecast risks, and train state-run AI models—which, alongside surveillance, were evidently the project's objectives from the outset.

It should also be noted that within the structure of Rosmolodezh, the deployment and management of chatbots falls under the purview of CISM—the very unit already actively monitoring social media, as mentioned in the previous section. It is well known that CISM maintains agreements with numerous law enforcement agencies and works in lockstep with the MVD, frequently flagging minors and young adults who publish content the authorities deem "banned" or "destructive."[155] Less widely known is that this same entity also recruits hackers. This came to light following cyberattacks targeting critical infrastructure in the European Union, Ukraine, and the United States, including transport systems, hospitals, tax authorities, courts, and banks. Investigations established that these attacks were directly coordinated by CISM Director General, Maxim Lupin, and his deputy, Mikhail Burlakov—actions that prompted Europol to place them on its wanted list.[156]

Nor should one overlook the fact that, in parallel with the tender for launching the "empathetic" chatbot, Rosmolodezh has announced its intention to "assist" regions in combating online "destructive content."[157] There is little doubt that these efforts are interconnected and that the chatbot system itself is conceived by its developers as an element of an overarching architecture of surveillance, propaganda, indoctrination, and predictive analytics embedded within the state's repressive apparatus.

---

[154] Ibid.
[155] Privin, Maksim. «Большой брат с функцией доноса. Как созданный Кремлем Центр изучения молодежи помогает возбуждать дела за комментарии в сети» [Big brother with a snitching function. How the Kremlin-created Center for Youth Studies helps initiate cases for comments online]. *vot-tak.tv,* March 12, 2026. https://vot-tak.tv/92037582/cism-monitoring-molodezhi (Accessed: 20.08.2026).
[156] Zatyrko, Andrey. «Раскрытая Евроюстом хакерская группировка оказалась связана с IT-структурой, созданной Путиным» [The hacker group exposed by Eurojust turned out to be linked to an IT structure created by Putin]. *Agents*, July 17, 2025. https://www.agents.media/raskrytaya-evroyustom-hakerskaya-gruppirovka-okazalas-svyazana-s-it-strukturoj-sozdannoj-putinym/ (Accessed: 20.08.2026).
[157] Denisenko, Anton. «Росмолодежь поможет регионам в борьбе с деструктивным контентом» [Rosmolodezh will help regions in the fight against destructive content]. *CNews*, May 6, 2026.

Central Control Room

The prominent manifestation of the state's drive to centralize educational platforms and school surveillance infrastructure is the "Unified Digital Education Monitoring System," officially launched by Rosobrnadzor on June 1, 2026. This system is designed to provide synchronized tracking of approximately 800 education-related metrics aggregated from various state agencies and databases.[158] Before reaching an official's screen, the students' daily academic performance and behavior are processed by algorithms and automatically converted into coefficients; these are then integrated into graphs based on the formulas of this rigid, top-down totalitarian machinery. Regardless of whether the current rudimentary version of this platform evolves into a real governance tool, as promised by officials, or fades into oblivion due to technical flaws, the initiative clearly demonstrates the authorities' ambition to assemble a unified, all-encompassing digital matrix. At its nexus sits a compact virtual control center where all key metrics converge. This represents an attempt to establish a level of surveillance reminiscent of the bleakest dystopias, where a handful of anonymous figures—with the push of a button, at their own discretion or even on a mere whim—can alter the destinies of millions of children and adults.

[158] Kommersant. «В России заработала единая цифровая система мониторинга образования» [A unified digital education monitoring system has become operational in Russia]. *Kommersant*, June 1, 2026.

Conclusion

Before our eyes, a radical restructuring of Russian schools is underway, transforming the educational environment into a new type of digital panopticon. Just 10 to 15 years ago, systems such as analog video cameras, internet monitoring, and online gradebooks were typically disconnected from one another, used different formats, and were confined to individual schools. If anyone attempted to weave these systems into a unified whole, it was usually the homeroom teacher, who did so with inherently human quirks, chasing after a couple of dozen students. This was a far cry from the "perfect" methods of automated big data processing, yet it left ample room for a humane, personalized approach. This state of affairs did not satisfy the central authorities, who resolved to fundamentally overhaul the data collection and processing infrastructure, making it unified, total, and vertical.

The Russian authorities have not merely introduced various new technologies, networks, and methods but have fundamentally altered the very mechanics of the old control architecture. At the core now lies the child's digital profile, within which previously unfathomable volumes of data are not only integrated but also subjected to correction, evaluation, and analytics. The homeroom teacher, once the individual who knew the child best, has been reduced to the lowest link in the surveillance chain. Relegated to the role of serving as just one of many data sources, the teacher's significance—with the expansion of new grading systems, educational resources, online classes, and video monitoring—is diminishing within an increasingly digital and pervasive matrix of control.

Schoolchildren's digital profiles are maintained in the FGIS "My School" and are also linked to the GIS "Prevention" when the authorities determine that a child requires special attention. These two systems are not isolated, static registries—one for schoolchildren and the other for disadvantaged families, runaways, deviant adolescents, and children in difficult life situations—but rather two dynamic elements of a unified digital state administration architecture. This architecture also encompasses neural networks, analytics programs, monitoring tools, hundreds of information platforms, thousands of databases, and countless applications. The weaving of this total control matrix allows the Russian regime apparatus to conduct and continuously refine the digital profiling of children. Its ultimate goal is the deployment of behavioral analysis, social scoring, automated rewards and punishments, algorithmic governance, and, ultimately, the education and upbringing of a completely predictable, malleable, and obedient population.

How far are the Russian authorities from building this dystopia? It is difficult to say, but one should avoid both overestimating and underestimating the situation. On the one hand, there are schools where internet access is merely nominal, the FGIS "My School" is filled out manually and irregularly by vice-principals, and video cameras remain analog, operating without recording capabilities. On the other hand, there are thousands of educational institutions where the situation

is reversed and predictive analytics has already been implemented. In light of this report, it is clear that the formation of a new Russian totalitarianism—where police batons are supplemented by neural networks—is progressing rapidly. Corruption, personnel shortages, poor infrastructure, interagency competition, sanctions, and mobile internet outages are slowing this movement but have neither stopped it nor turned it back yet. To verify this, one need only examine the rollout of the NSUD, the fate of the GosTech platform, or evaluate the latest capabilities and functions of the FGIS "My School" and the GIS "Prevention"—and then realize that, as recently as the late 2010s, all of this existed only in the plans of their developers.

The assembly of a matrix of total surveillance over children is being achieved not only through the rapid deployment of advanced technological platforms but also through governance reforms. The Ministry of Education's information systems have been transferred to the control of Mintsifry—the country's primary digital censor. Video surveillance in schools is no longer confined to school administrations or higher-level education authorities, with these data streams, routed through regional storage facilities, now fully accessible to the Russian National Guard, the MVD, and the FSB. All school network traffic is sifted through the infrastructure of Rostelecom, the main technical developer and operator of state surveillance systems, and Roskomnadzor, the principal internet watchdog. Moreover, regional authorities, Rosmolodezh, and the MVD, acting on Kremlin directives, are employing schools for extensive ideological investigations, organizing an online "hunt" for teenagers. This initiative involves both teachers, who are mandated to search for "destructive content" on students' social media accounts, and schoolchildren themselves, who are compelled to join cyber squads and participate in cyber-denunciations against their peers. The information gathered from this "hunt"—that is, data on what the authorities deem violations—is consolidated into a unified interagency platform, the GIS "Prevention," where MVD structures, becoming Russia's primary "educators," once again play a decisive role.

In closing, I must emphasize that investigating mass child surveillance systems highlights the urgent need for a radical alternative grounded in the principles of nonviolence, fairness, and respect for human dignity.

Sources Cited

Bibliography

Agents. «Крупнейший взлом российской цензуры: как она охраняет здоровье Путина, помогает Навке, заводит досье на журналистов и разводит ботов» [The biggest hack of Russian censorship: how it protects Putin's health, helps Navka, creates dossiers on journalists, and spawns bots]. *Agents*, February 8, 2023. https://www.agents.media/tsenzura/ (Accessed: 27.04.2026).

Alava, Jonna. "From Patriotic Education to Militarist Indoctrination—Disciplinary Power and Silent Resistance in Russia after the Onset of the War against Ukraine". Problems of *Post-Communism* 72, no. 5 (2025): 429–440.

Aleksandrov, Alexey. «В России начали широко рекламировать мессенджер Max. В чем его опасность и способен ли он стать аналогом китайского WeChat?» [In Russia, the Max messenger has begun to be widely advertised. What is its danger and is it capable of becoming an analogue of the Chinese WeChat?]. *Current Time*, 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: 23.08.2026).

Amnesty International. *"Only official sources" : Indoctrination in the Russian educational system*. Amnesty International, June 1, 2026. https://www.amnesty.org/en/wp-content/uploads/2026/06/EUR4609562026ENGLISH.pdf (Accessed: 15.09.2026).

Arkman, Arden. «Методичь. Как государственная пропаганда захватила российское образование — от детских садов до вузов» [Methodo-Madness. How state propaganda seized Russian education — from kindergartens to universities]. *The Insider*, October 10, 2025. https://theins.ru/obshestvo/284870 (Accessed: 20.08.2026).

Azattyq Asia. «В России запретили использовать телефоны на уроках в школе» [In Russia, the use of phones during school lessons has been banned]. *Radio Free Europe/Radio Liberty*, August 31, 2022. https://www.azattyqasia.org/a/32012530.html (Accessed: 19.08.2026).

Bakhur, Vladimir. «Эксперты: национальная система управления данными должна фокусироваться на пользе для бизнеса и граждан» [Experts: national data management system should focus on benefits for business and citizens]. *CNews*, November 29, 2018.

Belarusian Association of Journalists. «7 способов, которыми российский мессенджер Max следит за пользователями» [7 ways the Russian messenger Max tracks its users]. *Belarusian Association of Journalists*, October 7, 2025. https://baj.media/be/karysnae/max-sledit-za-polzovateljami/ (Accessed: 24.04.2026).

Bernard, Andreas. *Komplizen des Erkennungsdienstes. Das Selbst in der digitalen Kultur* [Accomplices of the Identification Service. The Self in Digital Culture]. Frankfurt am Main, S. Fischer Verlag GmbH, 2017.

CNews. «“Ростелеком” подключил к безопасному интернету более 47 тысяч школ и техникумов» [“Rostelecom” connected more than 47 thousand schools and technical colleges to secure internet]. *CNews*, February 28, 2023.

———. «Минцифры: приложением “Госуслуги Моя школа” пользуются более 12 млн человек» [Ministry of Digital Development: more than 12 million people use the “Gosuslugi My School” application]. *CNews*, September 1, 2026.

Colin, Alexander. “Mr. Nobody Against Putin gives an insight into the propaganda in Russian schools”. *The Conversation*, July 3, 2025. https://theconversation.com/mr-nobody-against-putin-gives-an-insight-into-the-propaganda-in-russian-schools-260162 (Accessed: 26.11.2025).

Daucé, Françoise, Benjamin Loveluck, Bella Ostromooukhova, and Anna Zaytseva. “From Citizen Investigators to Cyber Patrols: Volunteer Internet Regulation in Russia”. *Laboratorium: Russian Review of Social Research* 11 (3) (2020): 46–70.

Denisenko, Anton. «Росмолодежь поможет регионам в борьбе с деструктивным контентом» [Rosmolodezh will help regions in the fight against destructive content]. *CNews*, May 6, 2026.

Dietrich, Philipp. *The Key Player in Russia’s Cybersphere. What the West Needs to Know about VK Company.* German Council on Foreign Relations, September 20, 2023. https://dgap.org/en/research/publications/key-player-russias-cybersphere (Accessed: 18.08.2026).

Doroshenko, Darya. «В школах Сургута установили умные камеры с функцией распознавания лиц» [Smart cameras with facial recognition function have been installed in Surgut schools]. *Yugorsky Snegir*, August 21, 2025.

Dossier Center. «Глаза Кремля. Как устроен цифровой ГУЛАГ в России — и что мешает ему заработать в полную силу» [The Eyes of the Kremlin. How the digital GULAG is structured in Russia — and what prevents it from operating at full capacity]. *Dossier Center,* March 11, 2024. https://dossier.center/sorm/ (Accessed: 15.05.2026).

D-Russia. «Подписано соглашение об использовании решений “Московской электронной школы” при развитии ФГИС “Моя школа”» [A*n agreement was signed on the use of “Moscow Electronic School” solutions in the development of the FGIS “My School”*]. *D-Russia,* September 2, 2022.

———. «Счётная палата: 44,6% школ и колледжей считают недостаточной скорость Интернета для обучения» [Accounts Chamber: 44.6% of schools and colleges consider their Internet speed insufficient for learning]. *D-Russia*, June 26, 2025.

———. «Сервис для школ “Сферум” стал доступен из Max» [The “Sferum” service for schools became accessible from Max]. *D-Russia*, October 9, 2025.

Efremov, Gennady. «Некоторым россиянам хотят полностью запретить пользоваться сотовыми телефонами и смартфонами. Кого коснется» [Some Russians may face a complete ban on using cell phones and smartphones. Who will be affected]. *CNews,* March 25, 2026.

Enders, Anna, Lea Horne, and Marla Rivera. *The Max Messenger: An Analysis of Russia's State-Mandated Messaging Application*. InterSecLab, September 2026.

Galieva, Diana. «Госданные приглашают на платформу» [State data invited to the platform]. *Kommersant*, May 4, 2021

Gasparyan, Tat. «В дагестанских школах появится Wi-Fi и умное видеонаблюдение до конца 2025 года» [Wi-Fi and smart video surveillance will appear in Dagestani schools by the end of 2025]. *Kommersant*, June 3, 2025.

Goldenfein, Jake. *Monitoring Laws. Profiling and Identity in the World State*. Cambridge, Cambridge University Press, 2020.

HRW. «Россия: Школьников и студентов преследуют после протестов» [Russia: Schoolchildren and students targeted after protests]. *Human Rights Watch*, June 23, 2017. https://www.hrw.org/ru/news/2017/06/23/russia-children-students-targeted-after-protests (Accessed: 17.08.2026).

———. *Education under Occupation. Forced Russification of the School System in Occupied Ukrainian Territories*. Human Rights Watch, June 2024. https://www.hrw.org/sites/default/files/media_2024/06/ukraine_crd0624%20web_0.pdf (Accessed: 24.08.2026).

Kasmi, Elyas. «Власти собираются объединить все данные граждан и бизнеса в огромное электронное досье» [The authorities intend to combine all data of citizens and business into a huge electronic dossier]. *CNews*, November 30, 2018.

———. «Искусственный интеллект начинает контролировать поведение детей. Эксперимент поставят на российских школьниках» [Artificial intelligence begins to control children's behavior. The experiment will be conducted on Russian school children]. *CNews*, June 1, 2021.

Kelly, Catriona. *Children's World: Growing Up in Russia, 1890-1991*. New Haven, Yale University Press, 2007.

Kholupova, Kristina. «В московских школах установят тысячи видеокамер за миллиарды рублей» [Thousands of video cameras will be installed in Moscow schools for billions of rubles]. *CNews,* August 21, 2021.

Kinyakina, Ekaterina. «Умные камеры будут следить за российскими школьниками. Системой видеонаблюдения с функцией распознавания лиц оснастят все 43 000 школ» [Smart cameras will monitor Russian school children. A video surveillance system with facial recognition function will equip all 43,000 schools]. *Vedomosti,* June 15, 2020.

Kolomychenko, Mariya. «В России появится школьный реестр запрещенных сайтов» [A school registry of banned websites will appear in Russia]. *CNews*, April 17, 2014.

Kommersant. «В России заработала единая цифровая система мониторинга образования» [A unified digital education monitoring system has become operational in Russia]. *Kommersant*, June 1, 2026.

Korolev, Igor. «"Ростелеком" получит от властей 10 миллиардов на постройку интернета без Facebook, "Вконтакте" и танчиков» ["Rostelecom" will receive 10 billion from the

authorities to build an internet without Facebook, "VKontakte," and tank games]. *CNews*, August 3, 2020.

Korolev, Nikita, et al. «Контрольная по биометрии» [An exam on biometrics]. *Kommersant*, September 7, 2021.

Krasnushkina, Nadezhda. «Чиновникам предписана самоцифровизация» [Self-digitization mandated for officials]. *Kommersant*, October 18, 2018.

Kustov, Maksim. «В свердловских школах планируют внедрить ИИ для выявления девиантных подростков» [Sverdlovsk schools plan to introduce AI to identify deviant teenagers]. *Signal*, April 9, 2026.

Leo XIV, Pope. *Magnifica humanitas: On Safeguarding the Human Person in the Time of Artificial Intelligence* (Encyclical Letter). May 15, 2026. The Holy See. https://www.vatican.va/content/leo-xiv/en/encyclicals/documents/20260515-magnifica-humanitas.html (Accessed: 29.09.2026).

Litavrin, Maksim and David Frenkel. «Нейроскомнадзор. Чем пользуется РКН, чтобы следить за интернетом — и кто ему в этом помогает» [Neuroskomnadzor. What RKN uses to monitor the Internet — and who helps it in this]. *Mediazona*, February 8, 2023. https://zona.media/article/2023/02/08/grccc (Accessed: 10.08.2026).

Litoy, Aleksandr. «"Большой брат" от звонка до звонка. Как следят за соцсетями школьников» ["Big Brother" from bell to bell. How school children's social networks are monitored]. *Radio Free Europe/Radio Liberty*, December 22, 2019. https://www.svoboda.org/a/30338558.html (Accessed: 17.08.2026).

———. «Государство пришло в чат. Контроль над учителями, родителями и детьми» [The State has entered the chat. Control over teachers, parents, and children]. *Radio Free Europe/Radio Liberty*, November 30, 2023. https://www.svoboda.org/a/gosudarstvo-prishlo-v-chat-kontrolj-nad-uchitelyami-roditelyami-i-detjmi/32426381.html (Accessed: 17.08.2026).

Lugovskaya, Elizaveta. «За вашими детьми следят. Кто и зачем просит учителей мониторить соцсети учеников» [Your children are being watched. Who asks teachers to monitor students' social networks and why]. *Mel*, April 28, 2021.

Lukyanova, Irina. «Закон о хорошем поведении. Как и зачем депутаты опять отнимают у школьников телефоны» [The law on good behavior. How and why deputies are taking phones away from school children again]. *Novaya Gazeta*, November 7, 2023.

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

Lyubavina, Anna. «На развитие российской системы управления данными выделят почти шесть миллиардов» [Almost six billion will be allocated for the development of the Russian data management system]. *CNews*, March 7, 2025.

———. «Счетная палата: Выделенные на школьный интернет деньги потрачены неэффективно. Учителя говорят, что пользоваться сетью невозможно» [Accounts Chamber: Money allocated for school internet spent inefficiently. Teachers say it is impossible to use the network]. *CNews*, June 26, 2025.

———. «Школьников предлагают пересадить на специальные SIM-карты» [It is proposed to transfer school children to special SIM cards]. *CNews*, September 25, 2025.

Maleva, Yuliya. «Молодежь планируют нравственно обогащать через чат-боты» [They plan to morally enrich the youth through chat-bots]. *Vedomosti*, May 12, 2026.

Maleva, Yuliya and Tatyana Akinshina. «Минпросвещения разработает ГИС для профилактики детской преступности» [The Ministry of Education will develop a GIS for the prevention of juvenile delinquency]. *Vedomosti*, September 4, 2025.

Malgina, Anna. «"Господин Никто против Путина": как школьный педагог из Карабаша снял фильм, потрясший Запад. Интервью "Вот Так" с Павлом Таланкиным» ["Mr. Nobody against Putin": how a school teacher from Karabash made a film that shocked the West. An interview of "Vot Tak" with Pavel Talankin]. *vot-tak.tv*, June 3, 2025. https://vot-tak.tv/87052526/interviu-s-pavlom-talankinym (Accessed: 20.08.2026).

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

Mediazona. «Ростех: устанавливаемые в школах камеры не предполагают технологию распознавания лиц» [Rostec: cameras installed in schools do not involve facial recognition technology]. *Mediazona*, June 16, 2020. https://zona.media/news/2020/06/16/technology (Accessed: 20.08.2026).

Meduza. «Полиция по всей России покупает системы мониторинга соцсетей. Они помогают искать экстремизм "не выходя из рабочего кабинета"» [Police across Russia buy social media monitoring systems. They help search for extremism "without leaving the office"]. *Meduza*, October 16, 2018. https://meduza.io/feature/2018/10/16/politsiya-po-vsey-rossii-pokupaet-sistemy-monitoringa-sotssetey-oni-pomogayut-iskat-ekstremizm-ne-vyhodya-iz-rabochego-kabineta (Accessed: 15.05.2026).

———. «VK перешел под контроль Газпромбанка и "Согаза" друга Путина Юрия Ковальчука. Гендиректором VK станет сын Сергея Кириенко» [VK came under the control of Gazprombank and "Sogaz" of Putin's friend Yury Kovalchuk. Sergei Kiriyenko's son will 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: 19.08.2026).

———. «"Они могут начать противодействовать". Российские власти боятся детей, насильно вывезенных из Украины. Их пытаются «перевоспитать» и поставить под жесткий цифровой контроль» ["They may start resisting". The Russian authorities are afraid of children forcibly taken from Ukraine. They are trying to "re-educate" them and put them under tight digital control]. *Meduza*, March 11, 2024. https://meduza.io/feature/2024/03/11/oni-mogut-nachat-protivodeystvovat (Accessed: 20.08.2026).

———. «"Мы просто физически не успеваем вести свои обычные уроки". Как изменилось школьное образование в России за годы войны?» ["We simply physically do not have time to conduct our usual lessons". How school education in Russia has changed during the war years?]. *Meduza*, September 8, 2025. https://meduza.io/feature/2025/09/08/my-prosto-fizicheski-ne-uspevaem-vesti-svoi-obychnye-uroki (Accessed: 18.08.2026).

———. «Все иностранцы в России очень скоро окажутся под плотным контроля властей — на каждого человека составят максимально подробное досье» [All foreigners in Russia will very soon find themselves under tight control of the authorities — a most

detailed dossier will be compiled on each person]. *Meduza*, January 28, 2026. https://meduza.io/cards/vse-inostrantsy-v-rossii-ochen-skoro-okazhutsya-pod-plotnym-kontrolem-vlastey-na-kazhdogo-cheloveka-sostavyat-maksimalno-podrobnoe-dosie (Accessed: 04.09.2026).

———. «Вы наверняка слышали, что "Макс" шпионит за пользователями. Но вряд ли представляете, сколько разных инструментов для слежки внедрено в мессенджер Возможно, разработчики даже использовали нейросеть для прослушки» [You have probably heard that "Max" spies on users. But you hardly imagine how many different tracking tools are implemented in the messenger. Perhaps the developers even used a neural network for wiretapping]. *Meduza*, May 22, 2026. https://meduza.io/feature/2026/05/22/vy-uzhe-navernyaka-slyshali-chto-maks-shpionit-za-svoimi-polzovatelyami-no-vryad-li-predstavlyaete-skolko-raznyh-instrumentov-dlya-slezhki-vnedreno-v-etot-messendzher (Accessed: 22.05.2026).

Mel. «Губернатору Белгородской области пожаловались, что учителей заставляют мониторить соцсети школьников и заполнять по ним отчеты» [The Governor of the Belgorod Region was complained to that teachers are forced to monitor school children's social networks and fill out reports on them]. *Mel*, March 22, 2026.

Mikhalchenko, Elizaveta and Kseniya Mironova. «Школа хочет все знать о семье. В цифровую образовательную среду могут быть включены персональные данные учеников, учителей и родителей» [The school wants to know everything about the family. Personal data of students, teachers, and parents may be included in the digital educational environment]. *Kommersant*, June 19, 2019.

Mitrukhin, Sergey. «Видеокамеры в школах Новосибирска научатся распознавать драки и буллинг и отличать их от детских игр» [Video cameras in Novosibirsk schools will learn to recognize fights and bullying and distinguish them from children's games]. *Sibirsky Novostnoy*, August 27, 2025.

Novaya Gazeta Europe. «Свердловские власти начали мониторить соцсети школьников на предмет "запрещенного" контента» [Sverdlovsk authorities have begun monitoring school children's social networks for "banned" content]. *Novaya Gazeta Europe*, March 11, 2026. https://novayagazeta.eu/articles/2026/03/11/sverdlovskie-vlasti-nachali-monitorit-sotsseti-shkolnikov-na-predmet-zapreshchennogo-kontenta-news (Accessed: 19.08.2026).

Novye Izvestiya. «"Это - не слежка": в школах Екатеринбурга впервые в России установили прослушку» ["This is not surveillance": Audio surveillance introduced in Yekaterinburg schools for the first time in Russia]. *Novye Izvestiya*, April 7, 2022.

Ottinger, Lily. "China's AI Education Experiment". *ChinaTalk*, April 3, 2026. https://www.chinatalk.media/p/chinas-ai-education-experiment (Accessed: 06.08.2026).

OVD-Info. *Как власти используют камеры и распознавание лиц против протестующих* [How the authorities use cameras and facial recognition against protesters]. OVD-Info, January 17, 2022. https://reports.ovd.info/kak-vlasti-ispolzuyut-kamery-i-raspoznavanie-lic-protiv-protestuyushchih (Accessed: 19.08.2026).

———. *"The government's way or the highway": how the Russian authorities persecute teachers with an anti-war stance*. OVD-Info, January 30, 2025. https://reports.ovd.info/teachers (Accessed: 16.09.2026).

Petrova, Venera and Oleg Sapozhkov. «“Гостех”, раз-два» [“Gostech,” one-two]. *Kommersant*, September 22, 2025.

Petrova, Polina. «В школах Петербурга могут начать следить за поведением учеников с помощью искусственного интеллекта» [In St. Petersburg schools, they may begin to monitor students’ behavior using artificial intelligence]. *Peterburgskaya Gazeta*, March 19, 2026.

Poupin, Perrine. “Social media and state repression: The case of VKontakte and the anti-garbage protest in Shies, in Far Northern Russia”. *First Monday* 26 (5) (2021). https://firstmonday.org/ojs/index.php/fm/article/view/11711/11233 (Accessed: 18.08.2026).

Pozyachanyuk, Valeriya. «Операция “Детские ладошки”. Зачем “Сбер” собирает биометрические данные школьников» [Operation “Children’s Palms”. Why “Sber” collects biometric data of school children]. *The Bell,* October 7, 2020. https://thebell.io/operatsiya-detskie-ladoshki-zachem-sber-sobiraet-biometricheskie-dannye-shkolnikov (Accessed: 09.09.2026).

Privin, Maksim. «Большой брат с функцией доноса. Как созданный Кремлем Центр изучения молодежи помогает возбуждать дела за комментарии в сети» [Big brother with a snitching function. How the Kremlin-created Center for Youth Studies helps initiate cases for comments online]. *vot-tak.tv,* March 12, 2026. https://vot-tak.tv/92037582/cism-monitoring-molodezhi (Accessed: 20.08.2026).

RFE/RL. «“Насилие не остановить ни мониторингом, ни запретом соцсетей”. О попытках властей усилить контроль за школьниками в интернете» [“Violence cannot be stopped by monitoring or banning social networks.” On the authorities’ attempts to tighten control over school children online]. *Radio Free Europe/Radio Liberty*, February 17, 2026. https://www.svoboda.org/a/nasilie-ne-ostanovit-ni-monitoringom-ni-zapretom-sotssetey-o-popytkah-vlastey-usilit-kontrol-za-shkolnikami-v-internete/33680397.html (Accessed: 27.05.2026).

Roskomsvoboda. «Регионы заводят себе кибердружины» [Regions are establishing cyber squads]. *Roskomsvoboda*, October 9, 2019. https://roskomsvoboda.org/ru/50250/ (Accessed: 27.08.2026).

———. «Распознавание лиц внедрили в более чем 60 регионах России» [Facial recognition has been implemented in more than 60 regions of Russia]. *Roskomsvoboda*, October 24, 2023. https://roskomsvoboda.org/ru/post/syst-raspozn-62-region/ (Accessed: 20.08.2026).

Samsonova, Anastasiya. «“Ростелеком” укрепился в “Безопасном городе”» [“Rostelecom” strengthened its position in “Safe City”]. *ComNews*, June 6, 2019.

Savitskaya, Lyudmila. «Срочно удали лайк, иначе утром подают в полицию» [Delete the like immediately, otherwise they will file a report with the police in the morning]. *Radio Free Europe/Radio Liberty,* January 28, 2021. https://www.svoboda.org/a/31074785.html (Accessed: 26.05.2026).

Shi, Chen and Jianhua Xu. “Surveillance Cameras and Resistance: A Case Study of a Middle School in China”. *The British Journal of Criminology* 64, no. 5 (2024): 1150–1170.

Shvetsova, Anna. «Цифровой щит для ребенка. Что скрывается за идеей специальных детских SIM-карт» [Digital shield for a child. What lies behind the idea of special kids’ SIM cards]. *ComNews,* April 13, 2026.

Sizova, Nika. «“Гостех 2.0” будет работать на решениях провайдера облачных технологий Cloud.ru» [“Gostech 2.0” will run on solutions from cloud technology provider Cloud.ru]. *Vedomosti*, May 18, 2026.

Stepanova, Yuliya and Anastasiya Gavrilyuk. «Школьникам соберут портфолио. Российских учеников снабдят цифровым профилем» [A portfolio will be compiled for school children. Russian students will be provided with a digital profile]. *Kommersant*, June 8, 2021.

Strelnikov, Aleksey. «Мессенджер-шпион Max? Как россияне переходят на “максофоны”» [Spy messenger Max? How Russians are switching to “maxophones”]. *Deutsche Welle*, March 23, 2026. https://www.dw.com/ru/max-messendzerspion-pocemu-rossiane-perehodat-na-maksofony/a-76494140 (Accessed: 23.04.2026).

The Insider. «Минцифры предложило запретить детям получать SMS-рассылки. Операторы беспокоятся, что это может перекрыть им доступ к мессенджерам» [Ministry of Digital Development proposed to ban children from receiving SMS blasts. Operators worry this might cut off their access to messengers]. *The Insider*, August 7, 2026. https://theins.ru/news/295794 (Accessed: 25.08.2026).

Troitskiy, Konstantin. *Language Proficiency Testing for Foreign Children as a Tool of Russian Repressive Migration Policy*. Memorial Human Rights Defence Centre, 2026. https://memorialcenter.org/en/analytics/language-proficiency-testing (Accessed: 15.09.2026).

———. *The State Information Resource ‘Digital Profile of a Foreign National’ and the Shaping of a New Russian Totalitarianism*. Memorial Human Rights Defence Centre, 2026. https://memorialcenter.org/uploads/Konstantin_Troitskiy_The_State_Information_Resource_Digital_Profile_of_a_Foreign_National_and_the_Shaping_of_a_New_Russian_Totalitarianism_7b9d44affa.pdf (Accessed: 15.09.2026).

Uchitelskaya Rossiya. «Школы Новосибирска планируют оснастить камерами с ИИ для профилактики агрессивного поведения» [Plans to equip Novosibirsk schools with AI cameras to prevent aggressive behavior]. *Uchitelskaya Rossiya*, August 29, 2024.

Voronov, Aleksandr and Alexey Zhabin. «Детские лица сканируют для взрослых схем. В правительстве РФ рассказали, как может заработать биометрия в школах» [Children’s faces are scanned for adult schemes. The Government of the Russian Federation explained how biometrics in schools might work]. *Kommersant,* December 3, 2025.

Yale School of Public Health. *Forced Passportization in Russia-Occupied Areas of Ukraine*. New Haven, Humanitarian Research Lab at Yale School of Public Health, August 2, 2023.

Zakharov, Andrei. «“Умный город” или “Старший брат”? Как мэрия научилась знать о москвичах всё» [“Smart City” or “Big Brother”? How the Mayor’s Office learned to know everything about Muscovites]. *BBC News Russian*, April 10, 2020. https://www.bbc.com/russian/features-52219260 (Accessed: 17.09.2026).

Zatyrko, Andrey. «Раскрытая Евроюстом хакерская группировка оказалась связана с IT-структурой, созданной Путиным» [The hacker group exposed by Eurojust turned out to be linked to an IT structure created by Putin]. *Agents*, July 17, 2025.

https://www.agents.media/raskrytaya-evroyustom-hakerskaya-gruppirovka-okazalas-svyazana-s-it-strukturoj-sozdannoj-putinym/ (Accessed: 20.08.2026).

Documents and materials of Russian state authorities and municipal institutions

Analytical Center for the Government of the Russian Federation. «Национальная система управления данными. Концепция» (National Data Management System. Concept), Draft dated November 25, 2018, version 5.14 https://digital.msu.ru/wp-content/uploads/%D0%9D%D0%A1%D0%A3%D0%94.-%D0%9A%D0%BE%D0%BD%D1%86%D0%B5%D0%BF%D1%86%D0%B8%D1%8F_%D0%B28_25112018.pdf (Accessed: 20.04.2026).

Directive of the Department of Information Technologies of the City of Moscow dated July 31, 2015 No. 64-16-241/15 «Об утверждении регламента доступа пользователей...» (On approval of the regulations for user access...).

Directive of the Government of the Russian Federation dated April 30, 2026 No. 1030-r «Об утверждении комплекса мер...» (On approval of a set of measures...) https://www.consultant.ru/document/cons_doc_LAW_533626/ (Accessed: 17.08.2026).

Directive of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation No. 417, Ministry of Education of the Russian Federation No. 221 dated April 30, 2021 «Об утверждении требований к подключению и доступу...» (On approval of requirements for connection and access...) https://www.consultant.ru/document/cons_doc_LAW_388367/2ff7a8c72de3994f30496a0ccbb1ddafdaddf518/ (Accessed: 26.08.2026).

Directive of the Ministry of Education of the Russian Federation dated December 2, 2019 No. 649 «Об утверждении Целевой модели цифровой образовательной среды» (On approval of the Target Model of the Digital Educational Environment...) https://www.consultant.ru/document/cons_doc_LAW_341443/ad8f4e028380894173b4f017a56c42b4c5e4ad54/#dst100011 (Accessed: 13.08.2026).

Directive of the Ministry of Education of the Russian Federation dated December 17, 2019 No. R-135 «Об утверждении методических рекомендаций...» (On approval of guidelines...) https://www.consultant.ru/document/cons_doc_LAW_340889/ (Accessed: 21.08.2026).

Directive of the Ministry of Education of the Russian Federation dated June 30, 2021 No. 396 «О создании федеральной государственной информационной системы...» (On the creation of the federal state information system...) https://www.consultant.ru/document/cons_doc_LAW_395336/ (Accessed: 10.08.2026).

Directive of the Ministry of Education of the Russian Federation No. 232, Federal Service for Supervision in Education and Science No. 551 dated April 4, 2023 «Об утверждении Порядка проведения государственной итоговой аттестации...» (On approval of the Procedure for conducting the state final certification...) https://www.consultant.ru/document/cons_doc_LAW_447000/ (Accessed: 24.08.2026).

Directive of the Ministry of Education of the Russian Federation No. 233, Federal Service for Supervision in Education and Science No. 552 dated April 4, 2023 «Об утверждении Порядка проведения государственной итоговой аттестации...» (On approval of the

Procedure for conducting the state final certification...) https://www.consultant.ru/document/cons_doc_LAW_447215/ (Accessed: 24.08.2026).

Directive of the Ministry of Education of the Russian Federation No. 634, Ministry of Digital Development, Communications and Mass Media of the Russian Federation No. 925 dated September 8, 2021 «Об утверждении стандарта оснащения...» (On approval of the equipment standard...).

Directive of the Ministry of Labour and Social Protection of the Russian Federation dated April 3, 2023 No. 256n «Об утверждении Инструкции о порядке ведения...» (On approval of the Instruction on the procedure for keeping...) https://www.consultant.ru/document/cons_doc_LAW_447676/ (Accessed: 21.08.2026).

Directive of the School Principal of the Municipal Budgetary Educational Institution "Govzhinskaya Secondary General Education School" dated December 26, 2023 No. 166 «Положение о системе видеонаблюдения» (Regulations on the video surveillance system).

Directive of the School Principal of the Municipal Budgetary Educational Institution "Secondary General Education School No. 4 of Tosno" dated September 2, 2024 No. 450 «Положение о системе видеонаблюдения» (Regulations on the video surveillance system).

Directive of the School Principal of the Municipal Educational Budgetary Institution "Secondary General Education School No. 23 of the City of Taganrog" dated September 1, 2023 No. 458 «О создании и деятельности кибердружины...» (On the creation and activity of the cyber squad...) https://taganschool23.ru/2023-2024/Kiberdrujina/prikaz_o_sozdanii_kiberdruzhiny.pdf (Accessed: 17.08.2026).

Directive of the School Principal of the Municipal Educational Institution "Secondary School No. 25 of the Kirovsky District of Volgograd" dated April 23, 2025 No. 75 «О создании и функционировании Кибердружины» (On the creation and functioning of the Cyber squad) https://sosh25-vlg2012.ucoz.ru/food2/prikaz_o_sozdanii_kiberdruzhiny.pdf (Accessed: 18.08.2026).

Directive of the School Principal of the State Budgetary Educational Institution "Basic General Education School No. 21 of the City of Novokuybyshevsk, Samara Region" dated August 19, 2022 No. 104-OD «Об утверждении кибердружины...» (On the approval of the cyber squad...) http://nov21ooh.minobr63.ru/wp-content/uploads/2023/11/приказ-об-утверждении-кибердружины-буллинг.pdf (Accessed: 18.08.2026).

Directive of the School Principal of the State Budgetary Educational Institution of the Republic of Dagestan "RCO" dated August 30, 2021 No. 109 «Положение о системе видеонаблюдения» (Regulations on the video surveillance system).

Directive of the School Principal of the State Budgetary Educational Institution "Secondary General Education School No. 4 of Sunzha named after A.M. Kalimatov" dated September 1, 2022 No. 220/5 «Положение о системе видеонаблюдения» (Regulations on the video surveillance system).

Draft Resolution of the Government of the Russian Federation, prepared by the Ministry of Digital Development of the Russian Federation, project ID 02/07/07-26/00169086, as of July 6, 2026, «О внесении изменений в постановление Правительства Российской Федерации от 30 декабря 2024 г. N 1994» (On Amending the Resolution of the

Government of the Russian Federation of December 30, 2024 No. 1994) https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=PNPA&n=124111 (Accessed: 25.08.2026).

Federal Agency for Youth Affairs. Guidelines on preventing the spread of the ideology of terrorism, extremism and neo-nazism approved by the letter of Rosmolodezh dated February 27, 2025 No. GG/1449-06.

Federal Law of the Russian Federation dated December 29, 2010 No. 436-FZ «О защите детей от информации...» (On the protection of children from information...) https://www.consultant.ru/document/cons_doc_LAW_108808/ (Accessed: 12.08.2026).

Federal Law of the Russian Federation dated April 1, 2019 No. 48-FZ «О внесении изменений в Федеральный закон “Об индивидуальном (персонифицированном) учете...» (On amending the Federal Law “On Individual (Personalized) Record-Keeping”...) https://www.consultant.ru/document/cons_doc_LAW_321413/3d0cac60971a511280cbba229d9b6329c07731f7/#dst100031 (Accessed: 22.08.2026).

Federal Law of the Russian Federation dated December 19, 2023 No. 618-FZ «О внесении изменений в Федеральный закон “Об образовании...» (On amending the Federal Law "On Education...) https://www.consultant.ru/document/cons_doc_LAW_464808/ (Accessed: 17.08.2026).

Federal Law of the Russian Federation dated August 8, 2024 No. 303-FZ «О внесении изменений в Федеральный закон “О связи”...» (On amending the Federal Law "On Communications"...) https://www.consultant.ru/document/cons_doc_LAW_482565/ (Accessed: 28.08.2026).

Federal Law of the Russian Federation dated April 1, 2025 No. 41-FZ «О создании государственной информационной системы противодействия правонарушениям...» (On the creation of the state information system for countering offenses...) https://www.consultant.ru/document/cons_doc_LAW_502182/ (Accessed: 28.08.2026).

Federal Law of the Russian Federation dated June 26, 2026 No. 210-FZ «О внесении изменений в Федеральный закон “О связи”...» (On amending the Federal Law “On Communications”...) https://www.consultant.ru/document/cons_doc_LAW_537891/ (Accessed: 03.08.2026).

Instruction for Working with the Universal Library of Digital Educational Content (UB TsOK), Инструкция по работе с Универсальной библиотекой цифрового образовательного контента (УБ ЦОК). Portal myschool.eduprosvet.ru (Accessed: 14.08.2026).

Letter of the Federal Agency for Youth Affairs, dated February 27, 2025, No. GG/1449-06, «О направлении методических рекомендаций» (On Sending Methodological Recommendations) https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=871483 (Accessed: 11.09.2026).

Memo of the Ministry of Education of the Russian Federation and the Ministry of Digital Development, Communications and Mass Media of the Russian Federation, dated 2026, Памятка: Типовое облачное решение (ТОР) «Моя школа» (Internal regulations of federal IT implementation). Hosted on the official server of the Education Department of KUGO. https://obr-ku.ru/images/Documents/TOR/%D0%A2%D0%9E%D0%A0_%D0%9C%D0

%BE%D1%8F_%D1%88%D0%BA%D0%BE%D0%BB%D0%B0_%D0%9F%D0%B0%D0%BC%D1%8F%D1%82%D0%BA%D0%B0.pdf (Accessed: 12.09.2026).

Methodological Document of the Ministry of Education of the Russian Federation and the Ministry of Digital Development, Communications and Mass Media of the Russian Federation, Functional Capabilities of TOR. School // Brief Description of FGIS "My School" TOR. Education for the Regions of the Russian Federation (Функциональные возможности ТОР. Школа // Краткое описание ФГИС «Моя школа» ТОР. Образование для субъектов РФ), 2026. Hosted on the official server of the Government of the Smolensk Region. https://obrpoch.admin-smolensk.ru/files/561/tor_kratko_av.pdf (Accessed: 12.09.2026).

Official Communication of the Ministry of Education of the Russian Federation, dated November 14, 2025, «О разрешенном перечне интернет-ресурсов для использования в образовательном процессе» (On the Approved List of Internet Resources for Use in the Educational Process) https://www.consultant.ru/document/cons_doc_LAW_518910/ (Accessed: 25.08.2026).

Order of the Committee of Education and Science of the Kursk Region, dated May 20, 2021, No. 1-552, «Об организации в образовательных организациях Курской области мониторинга аккаунтов обучающихся в социальных сетях» (On the Organization of Monitoring of Students' Accounts in Social Networks in Educational Organizations of the Kursk Region).

Order of the Education Department of the Administration of the Ivanteevka Municipal District of the Saratov Region, dated November 10, 2022, No. 211, «О проведении мониторинга социальных сетей несовершеннолетних» (On Conducting Monitoring of Minor's Social Networks) https://uoivanteevka.ucoz.ru/sport/prikaz_o_prov_mon_socset_22.pdf (Accessed: 19.08.2026).

Order of the Education Department of the Tavda Urban Okrug of the Sverdlovsk Region, dated February 19, 2024, No. 109, «Об утверждении Порядка проведения мониторинга аккаунтов социальных сетей несовершеннолетних в образовательных организациях в новой редакции» (On Approval of the Procedure for Monitoring Social Network Accounts of Minors in Educational Organizations in the New Edition).

Order of the MBOU "Lyceum No. 1" of Dobrinka Settlement, Lipetsk Region, dated September 1, 2025, No. 386, «Приказ о мониторинге социальных сетей обучающихся» (On Monitoring of Students' Social Networks) https://lic1dobrinka.gosuslugi.ru/netcat_files/196/2998/Prikaz_o_monitoringe_sotsial_nyh_stey_obuchayuschihsya.pdf (Accessed: 19.08.2026).

Order of the MOBU "Secondary General Education School No. 23", dated September 1, 2023, No. 458, «О создании и деятельности кибердружины МОБУ СОШ № 23 в 2023-2024 учебном году» (On the Creation and Activities of a Cyber Squad of MOBU SOSh No. 23 in the 2023-2024 Academic Year) https://taganschool23.ru/2023-2024/Kiberdrujina/prikaz_o_sozdanii_kiberdruzhiny.pdf (Accessed: 17.08.2026).

Resolution of the Chief State Sanitary Doctor of the Russian Federation, dated September 28, 2020, No. 28, «Об утверждении санитарных правил СП 2.4.3648-20

"Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи"» (On Approval of Sanitary Rules SP 2.4.3648-20 Sanitary and Epidemiological Requirements for Organizations of Training and Education, Leisure and Health Improvement of Children and Youth) https://www.consultant.ru/document/cons_doc_LAW_371594/a87d3709aa01857b67d2d04477b1d8458572e62e/ (Accessed: 17.08.2026).

Resolution of the Government of the Belgorod Region, dated May 22, 2017, No. 181-pp, «Об организации деятельности кибердружин Белгородской области» (On the Organization of Activities of Cyber Squads of the Belgorod Region).

Resolution of the Government of Moscow, dated February 7, 2012, No. 24-PP, «Об утверждении Положения о государственной информационной системе "Единый центр хранения и обработки данных"» (On Approval of the Regulation on the State Information System Unified Center for Data Storage and Processing).

Resolution of the Government of the Russian Federation dated June 3, 2019 No. 710 (original version) «О проведении эксперимента по повышению качества и связанности данных...» (On conducting an experiment to increase the quality and connectivity of data...) https://ivo.garant.ru/#/document/77695224/paragraph/33:2 (Accessed: 17.09.2026).

Resolution of the Government of the Russian Federation dated June 3, 2019 No. 710 (as amended on November 17, 2025) «О проведении эксперимента по повышению качества и связанности данных...» (On conducting an experiment to increase the quality and connectivity of data...) https://ivo.garant.ru/#/document/72262102/paragraph/9093:5 (Accessed: 17.09.2026).

Resolution of the Government of the Republic of Buryatia, dated July 12, 2019, No. 378, «Об утверждении Порядка взаимодействия с кибердружинами в Республике Бурятия» (On Approval of the Procedure for Interaction with Cyber Squads in the Republic of Buryatia).

Resolution of the Government of the Novgorod Region, dated September 23, 2024, No. 457, «Об утверждении Регламента деятельности кибердружин в Новгородской области» (On Approval of the Regulations on the Activities of Cyber Squads in the Novgorod Region).

Resolution of the Government of the Russian Federation, dated November 24, 2014, No. 1240, «О некоторых вопросах по обеспечению использования сети передачи данных органов власти» (On Certain Issues of Ensuring the Use of the Data Transmission Network of Authorities) https://www.consultant.ru/document/cons_doc_LAW_171430/ (Accessed: 12.08.2026).

Resolution of the Government of the Russian Federation dated August 2, 2019 No. 1006 «Об утверждении требований к антитеррористической защищенности...» (On approval of requirements for anti-terrorist security...) https://www.consultant.ru/document/cons_doc_LAW_331342/ (Accessed: 30.07.2026).

Resolution of the Government of the Russian Federation dated May 14, 2021 No. 733 «Об утверждении Положения о федеральной государственной информационной системе...» (On approval of the Regulations on the federal state information system...) https://www.consultant.ru/document/cons_doc_LAW_384215/ (Accessed: 14.08.2026).

Resolution of the Government of the Russian Federation dated July 13, 2022 No. 1241 «О федеральной государственной информационной системе "Моя школа"...» (On the

federal state information system “My School”...) https://www.consultant.ru/document/cons_doc_LAW_422207/ (Accessed: 06.08.2026).

Resolution of the Government of the Russian Federation dated December 30, 2024 No. 1994 «Об утверждении Правил оказания услуг телефонной связи...» (On approval of the Rules for the provision of telephone communication services...) https://www.consultant.ru/document/cons_doc_LAW_495347/ (Accessed: 20.08.2026).

Resolution of the Government of the Russian Federation dated March 18, 2025 No. 318 «О государственной информационной системе мониторинга...» (On the state information system for monitoring...) https://www.consultant.ru/document/cons_doc_LAW_501497/ (Accessed: 25.08.2026).

Resolution of the Government of the Russian Federation dated April 1, 2025 No. 411 «О государственной информационной системе профилактики...» (On the state information system for prevention...) https://www.consultant.ru/document/cons_doc_LAW_502345/ (Accessed: 20.08.2026).

Resolution of the Government of the Russian Federation dated August 1, 2026 No. 962 «О внесении изменений в постановление Правительства Российской Федерации...» (On amending the Resolution of the Government of the Russian Federation...) https://www.consultant.ru/document/cons_doc_LAW_541441/ (Accessed: 12.09.2026).

Resolution of the Municipal Commission on Juvenile Affairs and Protection of Their Rights in the City of Nefteyugansk dated March 17, 2022 No. 11 «Об обеспечении информационной безопасности несовершеннолетних...» (On ensuring the information security of minors...) https://www.admugansk.ru/uploads/2023/02/%E2%84%96_11_ot_17.03.2022.doc (Accessed: 16.09.2026).

Resolution of the Government of the Russian Federation dated November 21, 2019 No. 2757-r «Об определении публичного акционерного общества “Ростелеком”...» (On determining the public joint-stock company “Rostelecom”...).

Resolution of the Government of the Russian Federation dated March 22, 2021 No. 713-r «Об определении публичного акционерного общества “Ростелеком”...» (On determining the public joint-stock company “Rostelecom”...).