2024

State of Surveillance

Research on how the Russian state, through laws and technology, carries out digital surveillance

Contents

Introduction

In this research we provide a brief top-level analysis of the current state of affairs of the governmental use of surveillance technologies in the Russian Federation. The research is devoted mainly to legal aspects and the enforcement of the existing legal rules by the law enforcers and governmental authorities, as well as their stance on the matter. We provide an overview of the existing legal framework governing the use of such technologies by the governmental bodies. In addition, we touch on the existing safeguards, transparency or oversight mechanisms to prevent the abuse of such technologies by the state agencies.

First, we provide an overview of the general laws empowering law enforcement agencies to resort to methods and technologies of collecting information relevant to the context of mass surveillance. Second, we list the number of specialised legal rules established by the federal laws that form legal regimes for various information service providers. Last, we focus on the ongoing deployment of facial recognition systems in public spaces. In addition, we refer to the relevant European Court of Human Rights (ECtHR) jurisprudence, highlighting issues of the Russian legal framework on the use of mass surveillance and breach of right to private life.

Sources

When carrying out a project and conducting research, we relied on both primary and secondary sources. Primary sources are original materials that provide direct evidence or first-hand information, such as federal laws, regulations, court cases, legislative bills and propositions. The first three will give an overview of existing legal bases, criteria, restrictions for the use of surveillance technologies, as well as safeguards against its potential abuse and the enforcement practices. The latter two will help us to demonstrate the dynamics and provide us with hindsight of the development of surveillance in the Russian Federation.

The research will also refer to interviews in order to highlight associated issues with the use of surveillance technologies in Russia.

Furthermore, we examine data from publicly available leaks from government sources engaged in surveillance, as well as affiliated organisations. Such information will not be interpreted on a stand-alone basis. We will compare it with the other sources to come to a conclusion on accuracy and credibility and make it clear what is known to be true, probably true, or untrue. Only the information that is already in the public domain, namely publicised in the internet media, will be used. Accordingly, we are not going to disclose insider information or seek access to such information by ourselves.

Secondary sources interpret or analyse primary sources. These sources include books and articles, including legal reviews that summarise, critique, or discuss the findings of researchers. Additionally, news articles of prominent media will be used to refer to the official position of the government and to the opinion of the experts from the relevant industries.

We also conducted online interviews with experts in electronic communications, information technology, infosec, and law to verify findings of the research. Each interview was conducted subject to written consent of the interviewee acquired beforehand. The consent addressed the citation policy preferable for each interviewee. The names of the experts are not disclosed for security concerns.

Legal framework related to the governmental surveillance activities

Russian Federation regulation is very different from that of the EU law and is generally viewed by practicing lawyers as extremely vague and susceptible to broad interpretation by the governmental authorities.

Below we list the laws that directly or indirectly relate to the matter discussed herein:

- Constitution of the Russian Federation adopted on 12 December 1993.
- Federal Law of 27 July 2006 No. 152-FZ “On Personal Data” (the “Personal Data Law”).
- Federal Law of 3 July 2003 No. 126-FZ “On Communications” (the “Communications Law”).
- Federal Law of 27 July 2006 No. 149-FZ “On Information, Information Technologies and Information Protection” (the “IT Law”).
- Administrative Court Procedures of the Russian Federation of 8 March 2015 No. 21-FZ.
- Russian Federation Code of Administrative Offences of 31 December 2001 No. 195-FZ.
- Federal Law of 2 February 2011 No. 3-FZ “On Police”.
- Federal Law of 17 January 1992 No. 2202-1 “On the Office of Public Prosecutor”.
- Federal Law of 12 August 1995 No. 144-FZ “On Operational-Search Activities”.
- Federal Law of 12 December 2022 No. 572-FZ “On the implementation of identification and (or) authentication of individuals using biometric personal

data, on amendments to some legislative acts of the Russian Federation and recognition of involved certain legislative acts of the Russian Federation" (the "Unified Biometrics System Law").

- Federal Law of 3 December 2008 No. 242-FZ "On State Genomic Registration in the Russian Federation".
- Federal Law of 24 April 2020 No. 123-FZ "On conducting an experiment to establish special regulation in order to create the necessary conditions for the development and implementation of artificial intelligence technologies in a constituent entity of the Russian Federation – the federal city of Moscow and amending Articles 6 and 10 of the Federal Law "On Personal Data"".

Legislation on the protection of privacy

The Constitution of the Russian Federation provides the right to privacy and to secrecy for communications; however, it does not contain any explicit provisions regarding personal data or any provisions directly related to digital rights. The rights to privacy and to access one's personal data have safeguards that are included in the Constitution.

First, Article 23, part 1 of the Constitution provides the right to the inviolability of private life, personal and family secrets, and the protection of one's honour and good name. In addition, part 2 specifically provides "the right to privacy of correspondence, of telephone conversations, postal, telegraph and other messages and its limitations are subject to court decision". The only provision that may be regarded as partially covering personal data processing is Article 24: "collection, keeping, use and dissemination of information about the private life of a person shall not be allowed without his or her consent". This Article also provides the right to information about the documents and materials of the governmental and local authorities directly affecting rights and freedoms, unless otherwise provided for by the law.

Similar general provisions regarding secrecy of communications are established by Article 63 of the Communications Law. This Article guarantees "secrecy of correspondence, of telephone conversations, postal, telegraph and other messages transmitted through telecommunications networks or post provided that it can be restricted by the federal law". It specifies the constitutional provisions by restricting "the inspection of postage by individuals who are not communications operator employees, seizure of postage, inspection of attachments, obtaining information and documents transmitted through telecommunications networks and post unless granted by the court decision or established in certain cases by federal law".

Concerning personal data protection, the key federal law regulating personal data processing is Federal Law of 27 July 2006 No. 152-FZ "On Personal Data". This

federal law was adopted in line with such international and supranational legal acts as the Organisation for Economic Co-operation and Development's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 "On the protection of individuals with regard to the processing of personal data and on the free movement of such data"; and the Council of Europe Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981. The latter one was signed and ratified by the Russian Federation. In 2018, Russia signed an Amending Protocol updating Convention No. 108. However, the federal data protection law was not amended and the law ratifying the Amending Protocol was not enacted.

Unlike the General Data Protection Regulation, the Personal Data Law is characterised by a broad scope as it covers both processing by private entities and individuals and by governmental authorities.

This basically means that general principles and legal rules are applicable to both for-profit or related to commercial activity processing and to the exercise of public functions by governmental authorities and local authorities (municipalities).

Article 6 of the Personal Data Law lays down general grounds for personal data processing. The most relevant to the scope of our research and applicable legal grounds that justify personal data processing in the absence of subject's consent are:

- The personal data being processed are related to an individual party to constitutional, criminal, administrative court proceedings, or commercial courts (arbitrage) proceedings.
- For achieving purposes stipulated by an international agreement of the Russian Federation or by the law, or for exercise and performance of functions, powers, and obligations imposed on personal data operators by the Russian Federation law.
- The personal data being processed are subject to publication or mandatory disclosure in accordance with federal laws.

In the course of court proceedings, the motion to disclose personal data or any non-public data is subject to judicial review. Article 63 of the Administrative Court Procedures of the Russian Federation of 8 March 2015 No. 21-FZ entitles parties to a trial to make motions before court to request evidence. Due to the broad scope of the listed provisions and provisions of the Personal Data Law listed earlier, it basically means that personal data can also be subject to such requests.

Similarly, Article 26.10 of the Russian Federation Code of Administrative Offences dated 30 December 2001 No. 195-FZ empowers government officers or agencies and judges to make requests for providing information necessary for administrative proceedings. However, such motions are subject to judicial review, meaning that by general rule, information requested (personal data) should be of relevance to a case tried. Nevertheless, we should draw attention that such administrative offence is somewhat similar to what constitutes petty crimes (eg speeding, littering, jaywalking) in some European countries.

Extrajudicial access to data

In the previous section, the legal grounds, namely mandatory disclosure or publication, also grant governmental authorities with extrajudicial access to personal data. Certain oversight or law enforcement bodies are able to access personal data without prior court decision.

The Prosecutor's Office

The Prosecutor's Office, which has also been recently vested with "censorship powers" by restricting access to websites on very vague and arbitrary grounds, is able to access personal data without prior court decision provided that such access is necessary for the oversight activities.

Article 4, part 2.1 of the Federal Law dated 17 January 1992 No. 2202-1 "On the Office of Public Prosecutor" explicitly empowers public prosecutors to access personal data, although only in the course of oversight activities.

The Order of Attorney General Office of 20 November 2013 No. 506 details certain provisions of the discussed law by providing a non-exhaustive list of personal

data that can be processed by the prosecutors in the course of prosecutor oversight measures.

However, prosecutor's oversight powers have a wide extent of issues to deal with. The Law "On the Office of Public Prosecutor" vaguely narrows down the discretion of prosecutors in exercising their oversight powers, as it does not provide an explicit exhaustive list of issues. On the one hand, it states that public prosecutors are responsible in general for ensuring compliance with laws of the Russian Federation. On the other hand, the same Law sets vague limitations of the purview. For example, pursuant to the Law, the prosecutors are specifically tasked to ensure the respect of human rights and freedoms and the compliance of investigatory bodies and law enforcement bodies performing operational-search activities with laws. Additionally, according to Article 21, part 2, prosecutors are not allowed to substitute their enforcement powers with those of the other law enforcement bodies. In other words, the oversight powers of prosecutors should not conflict with those explicitly vested in other governmental bodies by federal laws. Also, under Article 6, paragraph 2.3, prosecutors are not allowed to require documents or information not connected with the goals or subject-matter of the oversight. It practically means that prosecutors should refer to a specific federal law related to oversight. Last, but not least, prosecutors engage oversight measures if there is information about breach of law or infringement of human rights and freedoms obtained from persons or other governmental bodies.

Police

General provisions of police enforcement powers are provided by Article 13 of the Federal Law dated 2 February 2011 No. 3-FZ "On Police" which grants access to personal data. Article 13, part 1, paragraphs 3 and 5 specifically empower "police officers to access personal data in connection with the investigation of crimes, administrative offences, with investigative assessment of filed crime reports, administrative reports and incidents, or personal data of subjects related to mentioned above".

Article 6, part 1, paragraph 11 of the Personal Data Law provides a corresponding legal ground for personal data processing as mandatory disclosure established by the federal law. However, this Article of the Personal Data Law does not cover sensitive personal data (special categories of personal data in wording of the Russian legislation), as part 2 explicitly excludes from its scope processing of sensitive and biometric personal data.

Additionally, basing on the official construction of the Personal Data Law by the Ministry of Digital Development, Communications and Mass Media of the Russian Federation articulated in their informational letter of 17 July 2020 No. OP-P24-070-19433, Article 6 lists only general legal grounds. Articles 10 and 11, however, contain special legal grounds for the processing of sensitive and biometric personal data, respectively, that have a priority over the grounds established by Article 6 of the Personal Data Law. Under Article 10, personal data processing by the police or other law enforcement agencies can be deemed lawful if it is "necessary for the protection of life, health and other vital interests of personal data subject or that of the third-party or, for the establishment or enjoyment of personal data subject or third-party rights". It means that the police officers still have authority to access sensitive personal data; however, the legal threshold of its inquiries to be reasonable and justified is higher. For the biometric personal data, processing is lawful if it is provided by the federal laws specified in Article 11, part 2 of the Personal Data Law. Currently, only one of the federal laws listed in part 2 of the Article 11 contains

provisions regarding the processing of biometric personal data. The Federal Law of 3 December 2008 No. 242-FZ "On State Genomic Registration in the Russian Federation" provides for mandatory genomic registration of persons convicted and serving prison sentences for committing crimes, as well as suspects. In addition, from 1 January 2025, amendments to this law will come into force, according to which, among other things, persons subjected to administrative arrest will also be subject to mandatory genomic registration.

In other cases, we proceed from such an interpretation of the law that police officers are not formally authorised to request biometric personal data themselves because federal law does not expressly grant them such authority.

Nevertheless, a couple of reservations should be made here. First, such a view is based only on non-official construction of the Personal Data Law. Second, the scope of Article 13 of the Federal Law "On Police" is rather broad and refers mainly to such conventional police activities as enquiring and collecting information or documents in the course of investigatory assessments, retrieval of documents, and searches. The general character of Article 13 of the Federal Law "On Police" covers both extrajudicial access to personal data when such data do not fall under the protection provided by the Constitution or Law "On Communications" and access subject to preliminary court decision when personal data contain private information protected by these legal acts. In other words, in the course of various procedural actions, police officers can directly access data carriers containing, among others, biometric personal data or request such information directly from its owner. It is noteworthy that the fact of making such a request is not subject to confidentiality, i.e. any organisation possessing the data has the right to inform the person concerned about such requests, unless these requests are related to operational and investigative activities.

According to Article 13, paragraph 4 of the Federal Law "On Police", as well as Articles 6 and 7 of the Federal Law "On Operational-Search Activities", the police have the right to obtain all necessary information including personal data from any third

party, not only in the presence of a criminal case or a court decision, but also “in connection with the verification of statements and reports of crimes”, as well as in the presence of “signs of an unlawful act”, which seems to be a very vague concept. Nevertheless, the current system of requests for information obliges service providers to disclose any information requested by law enforcement authorities without the possibility to verify the existence of sufficient grounds and without any judicial control or oversight by an independent personal data protection authority.

Operational-Search Activities

The police officers as well as other similar law enforcement bodies and national security agencies (like the Federal Security Service [FSB]) have other legal grounds and ways to access communications data and personal data in particular.

The fundamental legislative act is Federal Law dated 12 August 1995 No. 144-FZ "On Operational-Search Activities", which provides law enforcement bodies empowered to conduct operational-search activities to collect and access information in general. According to the broad definition given in Article 1, operational-search activities are the type of activities, performed publicly or covertly, by the operative units of the governmental bodies authorised by this federal law within the limits of their powers, through the conduct of operational-search actions in order to protect life, health, human and civil rights and freedoms, and property, and to ensure the security of society and the state from criminal trespass. Article 6 lists exhaustively such operational-search actions as: surveys; inquiries; collection of samples for comparative research; controlled purchase; research of objects and documents; surveillance; identification of a person; inspection of premises, buildings, structures, areas, and vehicles; control of postal items, telegraph and other messages; wiretapping of telephone communications; interception of information from technical communication channels; operational infiltration; controlled delivery; operational experiment; and retrieval of computer information.

Formally speaking, Article 5 provides several provisions aimed at safeguarding human rights and freedoms. First of all, law enforcement bodies ensure privacy, personal and family secrets, inviolability of dwelling, and secrecy of correspondence. It also provides an individual with the right to appeal against operational-search activities against them to a superior law enforcement body, public prosecutor, or court. However, in order to effectively exercise this right in court, an individual should have at their disposal proof that operational-search activities were conducted against them, and criminal investigation against them was terminated on the grounds of the absence of criminal events or acts. An individual is entitled to obtain information collected about them in the course of operational-search activities subject to

confidentiality requirements and state secret. In case of refusal to perform or incomplete performance of such a claim by a law enforcement body (which is quite common), an individual is entitled to appeal to court. If the appeal succeeds, the court will order the enforcement body to provide the claimant with information collected about them during operational-search activities.

Additionally, Article 5 has data retention rules which prescribe to store data for one year and, after that, to erase information about individuals whose guilt was not established. Phonograms and other materials obtained by wiretapping are to be destroyed within six months, and if such materials were obtained under court decision, a relevant judge should be notified three months before the destruction. It is prohibited for officers to disclose, without an individual's consent, information affecting their privacy, personal and family secrets, honour, or good name discovered during operational-search activities. If the rights and interests of individuals or legal entities were infringed by a law enforcement body or an officer, a public prosecutor or a judge are obliged to undertake measures aimed to redress rights and interests and to award damages. Noteworthy in relation to mass surveillance is that there is an exhaustive list in Article 6 of such operational-search activities applicable to the use of IT solutions, including message control, wiretapping, access to computer information, and access to information from communication channels.

In accordance with Article 8, all operational-search activities interfering with the constitutional rights to secrecy of communication are allowed on the basis of court decision, provided that there is information about:

- Wrongful acts that require preliminary investigation, are being prepared or committed, or have been committed.
- Individuals preparing, committing or have committed wrongful acts that require under the law preliminary investigation.
- Events or actions (inactions) threatening to state, military, economic, information or environmental security of the Russian Federation.

However, in urgent cases that can lead to grievous or capital crime and if there is information about events, actions (inactions) threatening to state, military, economic, information or environmental security of the Russian Federation, it is allowed to conduct operational-search activities without preliminary court decision provided that a judge has been notified in 24 hours. After the beginning of such activities, a law

enforcement body is obliged to obtain a judicial decision within 48 hours to terminate such activities. Otherwise, in accordance with the federal law, failure to obtain the relevant court decision does not lead the outcome and findings of such activities to be erased, destroyed or rendered as inadmissible evidence in court.

Nevertheless, it is worth mentioning that according to Article 12.1 of the Law "On Operational-Search Activities", contents of the requests for information submitted in the course of operational-search activities are confidential, which means that a recipient of the request is not allowed to disclose its contents. In addition, Article 12 establishes that "information about means, sources, methods, plans, and results of Operational-Search Activities used or being used... organization and tactics of secret Operational-Search Activities is state secret and subject to disclosure only under the resolution of the relevant agency engaging Operational-Search Activities". In practice these two articles seriously impinge on the effective use of rights under Article 5 of the Law "On Operational-Search Activities" and constitutional rights provided in Article 24 of the Constitution. For example, Moscow City Court judgment 33a-0672/2021 dated 18.02.2021 rejected a claimant's appeal on a court decision of first instance. The claimant brought an action against Russian police who refused to provide him with information about operational-search activities conducted against him. The claimant sought to obtain confirmation about the mere fact of such activities, information about his character, confirmation about internal investigation against officers who disclosed information obtained during the course of operational-search activities, and to acquire copies of the relevant documents. An appellate instance, Moscow City Court upheld the court decision of first instance and denied appeal, as it reaffirmed that information requested by the claimant is protected under the aforementioned Article 12 and as a state secret.

To summarise, the provisions of the Law "On Operational-Search Activities" explicitly vests message control, wiretapping, access to computer information, and access to information from communication channels in police and national security agencies.

In other words, this Law grants powers to a number of law enforcement agencies to conduct operational-search activities and, consequently, powers to access communication data and to surveil over users and subscribers via information communication and technology. However, the provisions of the Law are very general in formulation and were elaborated in times when the majority of today's usual internet services did not exist or were in nascent phase of their development. That is why a number of federal laws and regulations exist to facilitate access to internet users or communication service subscribers' data in the course of operational-search activities. We are going to discuss them later.

Next, we provide an overview of legal provisions prescribing technical and organisational requirements for information dissemination organisers, communications service providers, and other information intermediaries and service providers to comply with.

To summarise, Russian laws granting enforcement powers to governmental authorities and regulating operational-search activities have the following characteristics:

Law "On Operational-Search Activities":

- Prohibiting disclosure of information about operational-search activities aimed to obtain personal data.
- The classified status (state secrecy) of information related to operational-search activities and their outcomes affects personal data subject rights to be informed about the processing of and access to their personal data.
- The current court practice and the classified status (state secrecy) renders individuals rights unenforceable in practice.

General laws, such as "On Police", "On the Office of Public Prosecutor", On "Personal Data":

- The existence of legal provisions granting access to personal data and other confidential information by governmental authorities without preliminary court authorisation.

Technical infrastructure

Digital service providers as agents of mass surveillance

The central law that endorses the so-called "new-school speech regulation" is the Federal Law of 27 July 2006 No. 149-FZ "On Information, Information Technologies and Information Protection" ("IT Law"). "New-school speech regulation" means a regulatory strategy when the government delegates some public or enforcement functions to information intermediaries and different service providers compelling them to strike down controversial content and to collect and retain data about their users. This law besides information restrictions sets a range of obligations for various service providers.

Currently the following service providers are compelled to engage in practices that might be regarded as surveillance (ranging by adverse impact on privacy from high to low):

- Information dissemination organisers (chats, forums, "in-house" comment section, messengers).
- Hosting providers.
- Social networks.
- Classified websites.

Noteworthy is that the recent amendment of 31 July 2023 to Article 8 of the IT Law introduced a requirement for all Russian online services to be accessible on condition of user authorisation via mobile phone number or through governmental systems such as USIA (Unified System of Identification and Authorization; in Russian: ЕСИА, also known as "Gosulugi") or Unified Biometrics System (UBS), or through any

other system (both governmental or private) provided it is not under foreign control. The same amendment also eliminated a pre-existing situation where hosting providers were one of the few online service providers that were not, as a general rule, legally obliged to engage in surveillance, for example there were no exhaustive rules of hosting service user identification.

Information dissemination organisers

The enactment of the Federal Law on 5 May 2014 No. 97-FZ (nicknamed as “Law on bloggers”) introduced Article 10.1 of the Federal Law of 27 July 2006 No. 149-FZ “On Information, Information Technologies and Information Protection” (“IT Law”) that compelled certain communication services – information dissemination organisers – to retain data of their users for six months.

In 2016, new amendments to the IT Law were introduced by the enactment of the Federal Law on 6 July 2016 No. 374-FZ (nicknamed after one of its sponsors as “Yarovaya package”), which extended the term of retaining users’ log data, ie metadata, up to one year, but left unchanged the six months term of retaining users’ content data (contents of users’ messages). Both types of data can be used to surveil users. However, while metadata provide mainly statistical and technical information about the user’s connection or device, content data contains messages itself, thus giving authorities not only information to trace, locate, or identify a person of interest through the use of metadata, but also to adduce these messages as proof against them.

In accordance with the IT Law, “information dissemination organiser” means a person who ensures functioning of information systems and (or) software products, designed and (or) used to receive, transmit, deliver, and (or) process electronic messages of internet users. Having reviewed the entries on such organisers from the relevant public records of the oversight agency, Roskomnadzor, as the source of the established practice, we can conclude that the discussed provision interpreted by Roskomnadzor is very broad and inclusive, including but not limited to virtually any web resources or applications that enable communication between its users. The resources sanctioned by Roskomnadzor include online maps or websites with commenting or posting functions, online classified ads services, bank applications with chat functionality, and instant messaging services.

Basically, Article 10.1 has an inadequately unrestricted scope that may potentially apply to any web resources with relevant functionality, disregarding their size, number of visitors, and ability to comply with the requirements established by the law. The broad character of the Article leads to arbitrariness in the governmental policies. Under Article 10.1, part 3.1, information dissemination organisers are obliged to "disclose information to law enforcement agencies in cases established by the federal law".

Currently, information dissemination organisers in accordance with Article 10.1, part 3 are obliged to store the following user data within the Russian Federation territory:

- Information about facts of receipt, transmission, delivery and (or) processing of voice information, text messages, images, sounds, video or other messages of internet users, and information about them within one year of completion of such actions (log/billing data).
- Text messages of internet users, voice information, images, sound, video or other messages of communication services users up to six months since their receipt, transmission, delivery and (or) processing (content data).

The details regarding the exact list of processed information are contained in the relevant acts of the Russian Government, namely Resolution of the Russian Federation Government of 23 September 2020 No. 1526 for log/billing data and Resolution of the Russian Federation Government of 26 February 2022 No. 256 for contents data. Both resolutions use the so-called nexus approach where the data retention rules are applicable only to users accessing through Russian infrastructure, namely resources, addresses, phone numbers, or users with documents issued by Russian authorities, or if metadata indicates that the user is located in the Russian territory. However, at the same time, both resolutions compel an information dissemination organiser, as defined in the law, to retain data of any user if law enforcement or national security agencies notify an information dissemination organiser that a user in question is

located in the Russian territory. Additionally, according to paragraph 13 of Resolution No. 1526, an information dissemination organiser has an obligation to ensure confidentiality about both the mere interaction with the national security agency and the subject of this interaction.

The main troublesome aspect of such interaction in the context of mass surveillance is that information requests issued by the authorities rely not only on routine requests for information but also on technical infrastructure designed to intercept and extract data transmitted through the service providers' infrastructure. Such technical capabilities of the authorities are ensured by Article 10.1, part 3 of the IT Law, which compels information dissemination organisers:

- To install surveillance hardware and software, to comply with relevant technical requirements, and to undertake measure to prevent disclosure of organisational and tactical methods of such installations.

- To disclose encryption keys (or any other information necessary for decryption) to the authorities, if an organiser uses additional encryption or provides users with such an option.

Technical capabilities of the surveillance equipment are described in the Order of the Ministry of Communications and Mass Media of the Russian Federation dated 29 October 2018 No. 571 (as amended by Order of the Ministry of Communications and Mass Media of the Russian Federation dated 28 August 2023 No. 750).

In short, the equipment, which is a part of the third generation System for Operative Investigative Activities (SORM), is designed to access all information mentioned in this subsection through communications channels during operational-search activities. SORM, which is a state-owned technical infrastructure, allows wiretapping and interception of communications, and is integrated into the networks of telecom operators and some IT service providers. In fact, SORM enables FSB officers remote, stable, effectively unsupervised, non-intermittent, with minimum latency (from 2 seconds up to 5 minutes for certain data) and round the clock access to information, as well as provides indirect and rather limited access for the other law enforcement bodies.

According to the Resolutions mentioned in this subsection it's only and

exclusively the FSB territorial departments that have remote access to such equipment. That's why, the police and other law enforcement bodies resort to a more common direct request of information approach, otherwise they have to cooperate with the FSB in order to get information they need. It should be noted that this equipment is only a part of the 3rd generation SORM (System of Operative Investigative Activity). SORM is a state-owned technical infrastructure that allows wiretapping and interception of communications, integrated into the networks of telecom operators and some IT service providers.

In case of information dissemination organisers, the motive behind the installation of this equipment is to provide the government with the ability not only to intercept communications made through landlines or mobile networks, but communications intermediated by different websites and messaging platforms.

As stated earlier, the definition of information dissemination organiser is rather broad, thus conditioning a great extent of discretion in enforcing Article 10.1. Currently, only services offering any communication functions, including, but not limited to, posting, commenting or chatting, fall under the scrutiny of the relevant oversight bodies. However, the risk that the scope of the Article is likely to be expanded still exists, because it depends greatly on the interpretation of the IT Law by Roskomnadzor.

The extent of the compliance with law depends on the location of information dissemination organisers and their informal relations with the government officials. Such information dissemination organisers as WhatsApp and Telegram do not comply with the requirements of the law, and are presumably reluctant to cooperate actively with the law enforcement agencies, as far as we can judge, based on the fact that WhatsApp is not even in the relevant public registry (there is a more convenient copy of the registry that is maintained and updated automatically by the civil rights advocate group Roskomsvoboda) and compliance with the law requires installation of the specialised equipment. From what is publicly available, it is highly unlikely that WhatsApp and Telegram purchased and installed such equipment locally in Russia. Finally, cooperation between WhatsApp and authorities might be unlikely from a political standpoint: the messaging app's parent company, Meta Inc., was declared as an extremist organisation and put into the relevant registries of the Ministry of Justice and Rosfinmonitoring in Russia. Moreover, the application of end-to-end encryption helps to conceal the contents of the messages from overreaching SORM and

significantly diminishes the value of potential cooperation between service providers and law enforcers. As far as we know, the decryption of messages is not possible and that is why law enforcement agencies resort to gathering metadata or logs of calls made through messaging services.

On the contrary, Russian information dissemination organisers have shown to be more cooperative with the law enforcement agencies, and they sometimes disregard procedural rules of processing legal requests for information from the law enforcement agencies. For example, social network and information dissemination organiser VK (Vkontakte) was reported to have flouted several times all the procedural rules and disclosed data of its users under a request that did not state probable cause and did not refer to an ongoing investigation of a crime or preliminary assessment of an incident. Endeavours to hold VK accountable ended up in the dismissal of the case. Moreover, there were a couple of instances which were reported when VK provided information acting on informal requests from the police sent via regular email.

Hosting providers

The most recent amendments to the IT Law introduced by the Federal Law of 31 July 2023 N406-FZ introduced new Article 10.2-1 which imposed new regulations specifically for hosting providers who had so far managed to avoid compliance with the requirements applicable to information dissemination organisers.

A hosting provider, according to the definition given in Article 2 of the IT Law, is a person providing computing power for uploading information into an information system constantly connected to the internet, e.g. GoDaddy Inc., Amazon Web Services. The requirements of the newly adopted provisions concern all hosting providers having nexus with the Russian territory either processing data of Russian users or receiving money from the Russian users or providing hosting services in the Russian market.

Article 10.2-1, parts 3 and 5 impose new obligations on hosting providers including the installation of surveillance equipment and the identification of hosting services users, respectively. Neither parts contain any details regarding its subject scope and technical requirements or even what data should be retained and the term of such data retention. It is the Order of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation dated 1 November 2023 No. 935 that sets a three-year term for the retention of data about their clients, namely the users (logs, billing, geolocation, personal data) of the hosting services;a one-day term for the retention of data about interactions of their hosting services clients with other internet users and describes technical capabilities of the surveillance equipment. It should be underlined that rules for the hosting providers are provided by Order No. 935, which is a piece of secondary legislation, unlike data retention rules established by the federal law for the information dissemination organisers. In other words, there is no need for the authorities to go through legislative rigmarole, thus, it is far easier and quicker for the authorities to change the scope and the term of data retention requirements for the hosting providers than for the information dissemination organisers.

Identification of hosting services users is detailed in the Resolution of the Russian Federation Government of 29.11.2023 No. 2011 and in addition certain additional methods of identification, it generally corresponds to Article 8 of the IT Law, as it prescribes that user identification and (or) authentication shall be made using Russian information or financial infrastructure.

In conclusion, the infrastructure and newly adopted relevant legal requirements contribute to the further development of the SORM system. Similarly, to the information dissemination organisers, the so-called control panels that enable the same unrestricted access to the information, as well as search and copy functions, are installed on the premises of the local departments of the FSB.

Telecommunication service providers – SORM

In this subsection, we are going to analyse wiretapping of telecommunications channels and surveillance over subscribers receiving telecommunications services from telecommunication providers operators, a legal entity, or an individual entrepreneur providing communication services under licence, such as mobile network or landline operators, internet access providers, satellite communications providers.

Article 64 of Federal Law of 3 July 2003 No. 126-FZ "On Communications" (the "Communications Law") provides a legal framework for the governmental authorities to access personal data through the telecommunication providers. Since 2016, when the Yarovaya package was adopted, under this Article, a communications operator is obligated to store on the territory of the Russian Federation:

- Information about facts of receipt, transmission, delivery and (or) processing of voice information, text messages, images, sounds, video or other messages of the users of communication services within three years of completion of such actions.
- • Text messages of communication services users, voice information, images, sound, video or other messages of communication services users for up to six months. The exact terms are set by the government.

Telecoms are obliged to cooperate with investigatory bodies by providing them with information about its users, rendered services, and other information. The technical infrastructure that enables wiretapping is SORM, which has gone through several generations.

SORM-1 was built in 1996 and enabled surveillance over telephone conversations. It involved installing devices into the infrastructure of a mobile or fixed-line operator that recorded telephone traffic and conversations and provided law enforcers with

access to these records.

SORM-2 was created to wiretap mobile communications and, of course, control the internet. SORM-2 is a system for storing information about internet traffic. It was developed in 2000 jointly by the Russian FSB and the predecessors of Roskomnadzor, but it was finally deployed only in 2008. It relied on special equipment installed on the provider's premises, and at their expense, which stores all traffic transmitted over the provider's networks and gives law enforcers access to this storage.

SORM 3, the most recent version, provides the integration of both of the previous systems. It includes additional control of some virtual private network servers, wiretapping Skype, communications data from encrypted messaging services (eg WhatsApp, Telegram, Signal), satellite communications, and a number of other features. However, access to messaging services using end-to-end encryption is restricted to metadata. The key result of SORM 3 implementation is that it brought the previous generations of SORM together. The main features are that SORM systems enable round the clock, real-time, indiscriminate access to communications data, including data about subscribers, the contents of messages unless encrypted, logging and billing data, and geolocation data.

Order of the Ministry of Communications and Mass Media of the Russian Federation 29 October 2018 No. 573 sets technical requirements for the whole SORM system and the scope of surveillance. Recent amendments from September 2023 included VoWiFi (voice over WiFi) and WiFi Calling in the scope of surveillance. Another regulation, Order of the Ministry of Communications and Mass Media of the Russian Federation 16 April 2014 No. 83, sets the rules of wiretapping internet communications via installation on the telecommunication providers side of special equipment aimed at gathering data about the connection (eg IP and MAC addresses, IMEIs) and the contents of user's messages.

The whole system enables law enforcement bodies to access almost all data transmitted through the telecommunication providers or communication channels without users' and service or telecommunication providers' knowledge.

This special equipment is functioning on a permanent basis (round the clock) automatically or on request and is unilaterally controlled by the FSB. The SORM system is designed to access information through communications channels in the course of operational-search activities that enables stable and non-intermittent access to information through telecommunications providers without the provider's knowledge.

However, the lack of regulatory safeguards as well as practical implementation of the system facilitates abuse of SORM. As we mentioned earlier, in the section describing operational-search activities, a person subjected to such activities has no legal redress to exercise his constitutional right for information because information about operational-search activities is a state secret and it is up to the law enforcement body to decide whether to disclose such information or not. The ability of the system to wiretap communications anytime makes existing court oversight almost ineffective and non-existent because FSB agents can use it anytime without having court authorisation, unless they want to adduce data from SORM as evidence for a criminal case, in which case they are still empowered to gather evidence without prior court authorisation.

One of our sources provided rather worrying details about the actual use of the system. SORM control panels that are installed on the FSB premises are rooted. In other words, FSB has full technical access to the control panel, meaning that FSB agents can delete and even modify log data and history of requests they made, thus aggravating the overall opacity of the surveillance conducted via SORM. This means that FSB agents can wiretap communications directly without filing a motion to receive court authorisation to do so. We asked the source about any internal measures of accountability or compliance in place. As our source explained, there is only a purely internal document that establishes the prosecutor's oversight over the use of the SORM system. However, as it has never been promulgated, its contents are unknown, as well as any instances when prosecutors interfered with use of the SORM system.

Regarding wiretapping in general and how different law enforcement bodies address the task of intercepting messages or collecting information about a person of interest, our source pinpointed three existing common scenarios. In the following paragraphs we present the information which they shared with us.

The first scenario is when FSB conducts their own operational-search activities using the SORM control panel by making separate targeted requests about users or actively wiretapping users communication channels. It is technical detachments of local FSB departments who engage in technical surveillance and operate SORM control panels. In general, there is an internal procedure when a regular agent files a formal request to a technical detachment, thus there is a theoretical possibility to trace surveillance activities. However, it was revealed to us that sometimes agents practice informal requests without complying with internal procedure – simply approaching agents from technical detachment and asking them to get certain information or to wiretap their objective or to have a look at the screen. Our source also noted that this is when root access to SORM control panel helps to conceal such informal requests.

The second scenario describes a situation when police officers conducting their own operational-search activities or investigation have access to communications information. Based on publicly available information, the technical capabilities of the Ministry of Interior Affairs are commonly assumed to be lower than those of FSB, which is why police officers usually have two options: they can either resort to cooperating with FSB in order to get information collected from the SORM, or they can directly request information from the telecommunication providers. In the latter case, it is not difficult to trace such activities because requests for information themselves are registered on both sides. In addition, in the latter case, there is always some latency as it takes some time to process requests and to execute them, which is why common requests for information cannot be an effective substitute for SORM. While it is quite obvious that thanks to the technical capabilities of SORM control panels, FSB agents have the most extensive access to communications data, police officers, for example, are reliant either on FSB when resorting to SORM or on the expertise of their own agents when drafting requests for information forwarded directly to telecommunications providers. In the latter case, it basically means that the depth and breadth of the request for information depends on the qualifications and experience of the police officer drafting the request. However, the expert drew our attention that there is such a practice when some police officers tend not to

comply with procedural requirements, and they sometimes establish unofficial or informal relations with corrupted telecommunications employees in order to illegally access data of their interest. Naturally, telecommunications companies do not publish transparency reports disclosing the number of requests for information as was stated earlier, even the mere request made during operational-search activities is subject to confidentiality requirements.

The third scenario partially conforms with the second one. The core motive of this scenario is the abuse of power not even to facilitate one's service, but to earn money on the side. This is the case when all the vices of the system are used, especially by police officers, to take bribes for shady services such as gathering information about cheating spouses, competitors, or potential victims of blackmailing. Sometimes they do not have direct contact with the instigators of such unlawful acts, but with intermediaries such as private detectives or employees of security companies or internal security staff, who are quite often former police officers or law enforcement agents themselves. Naturally, officers do not comply with procedural requirements and do not execute documents that may trace back their illegal activities. In this scenario, SORM is highly unlikely to be used by police officers and that is why they use their informal contacts among telecommunication providers to glean information of their interest, or they use different web services.

The full-scale wiretapping involving the first scenario is more often used only against high-profile cases, both criminal or political, due to time and cost concerns. A source clarified that law enforcement officers, namely police officers, when persecuting individuals for exercising freedom of speech or assembly, rely more on gathering of metadata, which eventually helps them to approximate the location of the user's device and consequently a user themself. After that, police officers conduct common field activities like searches or visits to the supposed locations of the users. The source noted that wiretapping and interception of contents data is rarely, if ever, practised in such cases.

In its own way: SORM and international law

In 2015, the ECtHR voted unanimously in its judgment Roman Zakharov v. Russia that the right to privacy, guaranteed by Article 8 of the European Convention on Human Rights of 1950, was violated and found that the Russian domestic legal provisions governing the interception of communications did not provide adequate and effective guarantees against arbitrariness and the risk of abuse.

The Court ruled that the domestic law did not meet the “quality of law” requirement and was incapable of keeping the “interference” to what was “necessary in a democratic society” (paragraph 304). Despite the fact that the judgment was handed down related to mobile telephone communications surveillance, conclusions of the Court are still relevant today and parallels can be drawn to internet communications surveillance as both types of secret surveillance share the same legal framework (federal legislation) and are performed by the same law enforcement agencies.

The Court found that the risk of abuse inherent in any system of secret surveillance was particularly high in Russia where the secret services and the police had direct access, by technical means, to all mobile telephone communications. In particular, the Court found shortcomings in the legal framework in the following areas: the circumstances in which public authorities in Russia are empowered to resort to secret surveillance measures; the duration of such measures, notably the circumstances in which they should be discontinued; the procedures for authorising interception as well as for storing and destroying the intercepted data; and the supervision of the interception (paragraph 302).

Moreover, the effectiveness of the remedies available to challenge the interception of communications was undermined by the fact that the claimants were unable to submit proof of interception.

This derives from Article 5 of the Law "On Operational-Search Activities" and that obtaining such proof was impossible in the absence of any notification system or possibility of access to information about interception due to its classified status.

To conclude, this ECtHR ruling established that legislation and practices of the Russian Federation have the following characteristics:

- Domestic law is not clear enough to give persons an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to secret surveillance operational-search activities and not to other less intrusive activities.
- The necessity and proportionality principle is not observed as legislation, namely the IT Law and Communications Law, authorise, on a generalised basis, storage of all personal data of all the persons without an objective criterion being laid down in the legislation by which to determine the limits of the access of the public authorities to the data and of its subsequent use, for purposes which are specific, strictly restricted, and capable of justifying the interference that both access to the data and its use.
- Lack of independent oversight mechanism. Persons are entitled to file a complaint to the law enforcement agency under Article 5 of the Law "On Operational-Search Activities".
- Effective remedies are not available to an individual, as de jure existing right to lodge a complaint against operational-search activities to the agency in breach or to file a suit if personal data were obtained in the course of operational-search activity will not upheld by the court, as an individual cannot obtain evidence to support their allegations and to redress their rights in an effective manner.

The findings of the ECtHR in the case of Roman Zakharov v. Russia demonstrates that the Russian legal framework, which condones the widely accepted practice of covert mass surveillance over communications, violates Article 8 of the European Convention on Human Rights of 1950. Furthermore, the same legal framework does not efficiently restrict access of public authorities to communications data to the extent necessary and proportionate in a democratic society and does not provide data subjects with effective (enforceable) redress.

In conclusion, it is noteworthy that the Russian Government not only refused to implement the critical findings of the ECtHR, but the Federal Assembly (the Russian parliament) enacted the federal constitutional law empowering the Russian Constitutional Court to determine whether it is possible to execute the decision of any intergovernmental body on human rights and freedoms if there is an uncertainty about its compliance with the Constitution.

Another notable case of the ECtHR regarding the use of SORM by the governmental authorities is Podchasov v. Russia (Telegram encryption keys case), which specifically dealt with the legal requirements for the information dissemination organisers established by Article 10.1, part 3 of the IT Law, namely to install surveillance equipment that ensures access to data and to disclose encryption keys to FSB. This decision of the ECtHR was based on Roman Zakharov v. Russia because the legal framework for secret surveillance and its implementation, as the ECtHR acknowledged, are the same for both telecommunications service providers and information dissemination organisers (paragraph 55).

Again, the ECtHR voted unanimously that the right to privacy, guaranteed by Article 8 of the European Convention on Human Rights of 1950, was violated. The Court noted that the contested provisions pursued a legitimate goal, but the contested legislation was not necessary in a democratic society. The lack of legal safeguards, such as the absence of legal requirement for the law enforcers "under domestic law to show the judicial authorisation to the communications service provider before obtaining access to a person's communications" (paragraph 72), and the obligation to install hardware equipment that enables direct remote access to all internet communications and related communications data, underpinned the argument that such interference is not necessary in democratic society. The ECtHR concluded that "the Russian [legal system], which enables the secret services to access directly the internet communications of each and every citizen without

requiring them to show an interception authorisation to the communications service provider, or to anyone else, is particularly prone to abuse" (paragraph 73). Dealing with the provision requiring information dissemination organisers to decrypt data, the Court concluded "that in the present case... the statutory obligation to decrypt end-to-end encrypted communications risks amounting to a requirement that providers of such services weaken the encryption mechanism for all users; it is accordingly not proportionate to the legitimate aims pursued" (paragraph 79). The Court posited on the fact that there is no technically feasible opportunity to ensure discriminate access to encrypted messages, ie access to specific Telegram users of interest; instead, the Russian legal framework embraced the opposite: indiscriminate access to messages and other data of all users by attempting to weaken encryption for all users (paragraph 77).

Biometrics and facial recognition

Currently, there are no federal laws that explicitly regulate governmental use of facial recognition or state-wide facial recognition system, although there are initiatives to create state-wide base infrastructure and toolkits for other regions of the Russian Federation that help local authorities to deploy facial recognition systems.

The legal grounds of using facial recognition in public spaces are not explicitly set by federal law. On the one hand, Article 11, part 1 of the Personal Data Law contains a general legal prohibition of the processing of biometric personal data without personal data subject consent. On the other hand, Part 2 provides an exhaustive list of derogations when biometrics processing might be used without personal data subject's consent. Currently, the government seems to be reliant on a couple of derogations in order to implement mass surveillance using artificial intelligence/machine learning (AI/ML) technologies coupled with biometrics processing. These derogations are counter-terrorism and transportation security. However, the relevant federal laws have neither any explicit provisions regarding biometric personal data, nor explicit derogations to empower the government to process biometric personal data pursuant to these federal laws. There are several instances mentioned here that there is an effective de facto use of facial recognition technologies in transportation and in certain public schools. In the latter case, it is only public sports schools, as well as sports facilities in general, that have the so-called objects of high terrorist attack risk on the premises which can lead to more than 101 casualties (eg stadiums, swimming pools, and other similar facilities) that must be equipped with facial recognition systems.

Facial recognition: an ongoing regulatory experiment

Another piece of federal legislation that implicitly provides legal grounds for the local use of facial recognition is Federal Law of 24 April 2020 No. 123-FZ "On conducting an experiment to establish special regulation in order to create the necessary conditions for the development and implementation of artificial intelligence technologies in a constituent entity of the Russian Federation – the federal city of Moscow and amending Articles 6 and 10 of the Federal Law "On Personal Data"." This Law empowers implicitly authorities of the federal city of Moscow to use facial recognition technologies on the territory of Moscow.

Namely, Article 4, part 1, paragraph 5 of the Law might be characterised as setting the mandatory information disclosure requirements by empowering the executive local authorities: "*to establish procedure and cases when owners of photo and video surveillance equipment and systems should transfer images obtained in accordance with the conditions provided for in subparagraphs 1 and 2 of paragraph 1 of Article 152.1 of the Civil Code of the Russian Federation (images of individuals made in public interest or in public spaces or events), as well as provide access to such photo and video surveillance equipment and systems to government bodies and organizations performing public functions in accordance with regulatory legal acts of the Russian Federation*". Currently, there is no definite single rule for such transfer and provision of access or a defined purpose, leaving much freedom of action for the governmental bodies. According to the Resolution of 3 December 2020 No. 2136-PP adopted by Moscow Government, this interaction is executed on a case-by-case basis subject to conditions set out in the compacts between the Department of Information

Technologies of Moscow Government and the owners of photo and video surveillance equipment. In addition, this Resolution requires all image transfers and provision of access to be made via the Unified Center of Data Storing, the governmental information system.

It is noteworthy that such processing of personal data (images) does not contradict strictly the general prohibition set by Article 11 of Personal Data Law. In fact, mere images of individuals are not considered to be biometric personal data unless they are used for identification of a personal data subject. This interpretation derives from the law itself, namely from the definition of biometric personal data given in Article 11, part 1 of the Personal Data Law, and is fully supported by the oversight bodies, the Ministry, and by court practice.

Even in the Moscow region, the overall process of adopting and implementing facial recognition technology took quite a time. The local authorities had been creating relevant infrastructure for years, before the mere testing of facial recognition technologies became possible. For example, during this period, in 2012, Moscow authorities established a Unified Data Storage and Processing Center (in Russian: Единый центр хранения данных, ЕЦХД), a central video data storage with remote access to cameras and archives in real time.

From 2016 to 2018, facial recognition technology was tested as part of the development of urban public safety programmes, including preparation for the World Cup which was hosted across Russia in 2018. Given the available public statements made by top government officials, city-wide implementation of AI seems to have begun at some point in 2019 (see Table 1).

The city also implemented the Safe City Program which integrated on a single platform all the systems responsible for public transportation security, police databases, and the information systems of the Ministry of Health and the Ministry of Emergency Situations, as well as regional, administrative district-level, and municipal district-level systems.

Table 1 – Brief chronology of video surveillance development leading up to the Moscow AI experiment

2001	Black and white cameras in residential buildings and public spaces
2005	Cameras connected to video surveillance points
2007	Safe City Program launched
2010	Moscow Department of Information Technology created; new mayor Sergey Sobyanin appointed
2011	Unified Data Storage Center created; growth of protests
2012	Ban on hiding face at rallies
2014	Scaling of the Safe City Program
2015	Anti-terrorist security measures for 2018 FIFA World Cup
2016	NtechLab introduced FindFace technology
2017	Moscow Department of Information Technology collaboration with NtechLab launched
2018	Face recognition for 2018 FIFA World Cup tested
2019	Collaboration of Sberbank and the Moscow Government
2020	Experiment with AI launched; surveillance used to track citizens during the Covid-19 pandemic
2021	UBS acquired the status of GIS (state information system), state monopoly for biometric data
2022	Technology has been used against protesters and those fleeing military mobilisation

The row for 2022 was added by Privacy International. For the original table and a more detailed analysis of facial recognition development, see: Ross, S., Serebrennikov, D., Miaeva, E. and Netyaev, V. (2024) Surveillance technologies in autocratic regimes: the Moscow AI experiment and its implications for crime control and police effectiveness, SSRN.

The so-called legal experiment with the city-wide use of AI/ML began in 2020. City-side deployment of the technology coincided with the Covid-19 global pandemic. In January 2020, the Moscow Government procured facial recognition technologies from NtechLab (partially owned by state corporation Rostec), VisionLabs (a subsidiary of Sberbank), and Tevian. At the end of 2020, the Moscow Government enacted several resolutions that formally legalised the use of AI/ML technologies in the Moscow city region and ensured the in-flow of image data from private video surveillance systems (see: ResolutionI of the Moscow City Government of 3 December 2020 No. 2136-PP "On the procedure and cases of transfer of images by owners of means and systems of photo and video surveillance, as well as providing access to means and systems of photo and video surveillance in order to create the necessary conditions for the development and implementation of artificial intelligence technologies in the city of Moscow" Bulletin of the Mayor and Government of Moscow, No. 69, 15 December 2020). However, none of the Moscow Government resolutions explicitly addressed the use of AI for facial recognition.

Several major political rallies took place in Moscow with the common feature that many participants were detained after leaving the rally. According to OVD-Info, 212 people were detained at a rally on 23 January 2021, and about 100 people were detained in the week after. In total, OVD-Info recorded at least 454 detentions ex post facto in 2021. Of these, 363 were related to a rally on 21 April. At least 164 people noted that during their encounter with the police or during the court hearings, they were told about the use of photo and video materials as court evidence.

Today, there is an assumption that all closed-circuit television (CCTV) cameras in the Moscow transport infrastructure and a significant share of cameras in public streets are connected to the Unified Center of Data Storing. In the Moscow Metro, facial recognition systems are used in law enforcement activities and for contactless payments. The former system is officially nicknamed "Sphere". Additionally, in April 2023, the Military Commissar for Moscow claimed that facial recognition was used to search for conscripts. In addition to the Moscow transport infrastructure and streets, the local government planned to launch facial recognition in Moscow's public schools.

The main troubling aspect of the use of facial recognition in Moscow is that the procedure of gathering reference images is completely opaque, as well as its subsequent use for identification. Such reference photos can be gathered

automatically from the users' profiles registered with the website mos.ru, as the development of such functionality was procured by the local government. Moreover, due to the general prohibition of the processing of personal data, of which authorities are aware, they have to resort to interpretation contrivances and formalities in order to avoid obligation to comply with the law. Such a formality was revealed in the Alena Popova case of 2019.

At the end of 2018, Alena Popova held a single picket near the State Duma demanding the resignation of deputy Leonid Slutsky, who allegedly sexually harassed several journalists. For this act, she was held liable to an administrative fine of 20,000 rubles (approximately 220 USD, 173 GBP). In her case, the prosecution adduced images from a video surveillance camera analysed with facial recognition technology. In 2019, Popova attempted to challenge the use of images captured by public video cameras and the application of facial recognition technology. She filed an administrative lawsuit against the Main Administration of Ministry of Internal Affairs and Department of Information Technologies of Moscow City Government, but eventually both the first instance court and appellate court dismissed her case. Omitting the reasoning of the court regarding the use of mere images of individuals (ie raw images without any additional information), it was the explanation furnished by the local authorities that there was no processing of biometric personal data, which eventually underpinned dismissal of the case. The court just reasserted the legal position of the Moscow Government: "*The facial recognition algorithm used by the UCDS [Unified Center of Data Storing] compares the image received by the UCDS from video cameras with a photograph provided by a law enforcement agency. In the process of processing the corresponding images, they are compared for the presence or absence of matches. The Department does not transfer personal data (full name, etc) of the persons sought, since the Department does not have the technical and legal ability to compare them.*"

Popova lodged an application before the ECtHR challenging the legality of facial recognition technology.

In other words, the official stance of Moscow authorities supported by the court is that the Unified Center of Data Storing and Processing does not process biometric personal data of citizens or identify persons in images. According to the Moscow Government, when comparing images of individuals captured in public spaces, they use facial recognition technology only for 1-to-1 authentication, namely to find a

match to an image provided by the police among other images of individuals stored in the Unified Center of Data Storing and Processing. In addition, it should be noted that it is not the Unified Center of Data Storing and Processing which performs facial recognition, but rather it serves as a central storage for all the images captured from video cameras in the streets. It is PARSIV (Subsystem for Automatic Registration of Scenarios for Indexing Video-information; in Russian: ПАРСИВ), an IT solution integrated with the Unified Center of Data Storing and Processing of Moscow city, that performs facial recognition and finds matching images. At its core, PARSIV is a gateway through which police officers can connect to the city's facial recognition system to search for suspected criminals.

After the last upgrade of the system in 2021, police officers can apply many filters to search for a person: gender, age, race, glasses, beard, mask, headdress, and the ability to recognise silhouettes. PARSIV allows you to track a person's route in a given area. The system is under the jurisdiction of the Moscow Government, namely the Department of Information Technology, which grants access to PARSIV to various other agencies, including law enforcement ones.

We believe that even if there is a procedure and some regulation of the issue in question, it is not subject to any public control or court oversight. The absence of explicit regulation on the use of facial recognition, its admissibility as court evidence, and the overall opacity of relevant procedures contribute to the abuse of police access to the database and to the existence of black data market.

The first signs that city-wide facial recognition would succumb to the corruption and abuse of power appeared on the radar in 2019. Back then, only 3,000 city cameras were providing images for the facial recognition system as part of the test. According to the findings of an investigation made by Andrei Kaganskikh, it was possible to buy day access to public video cameras (live or archive) or to track a person by finding matches with the provided image.

In September 2020, Anna Kuznetsova, a Roskomsvoboda volunteer, purchased on the internet for 16,500 rubles (approximately 218.88 USD or 167.67 GBP based on the average exchange rate of Bank of Russia in June 2020) a pdf file with images from city surveillance cameras. The file contained a total of 70 images of her face, with an accuracy of 71%, and the addresses where they were captured. Officers of the Internal Security Administration of the Ministry of Internal Affairs conducted its own

investigation and confirmed the allegations using a “controlled purchase” tactic with the help of two volunteers. As a result, the Investigative Committee of Russia opened a criminal case on the facts of abuse of power and violation of privacy (Article 285 and Article 137 of the Criminal Code of the Russian Federation, respectively). The perpetrators proved to be two police officers. One who served in the Center of Operational-Search Information of the Administration for North East Administrative District of Moscow of Ministry of Internal Affairs and had direct access to PARSIV. The other was a patrol officer from a local police department, who acted as an intermediary between the actual doer and persons who were interested in accessing information from the databases. According to the court case materials publicly discussed in the press, Dmitry Golovin, head of the city video surveillance department in the Department of Information Technology, who was interrogated as a witness in the case, told investigators that law enforcers have the right to receive anonymised authorisation data to access PARSIV. It was reported in the media that he had added that this process is supported by a large number of agreements, regulations, and amendments, which clearly define the procedure for access to data, and which state that disclosure of this information to third parties is strictly prohibited. However, we did not find any promulgated regulations or publicly available official documents detailing such interaction. Noteworthy, it was also reported in the media that Alexander Kulik, a chief officer of the Center of Operational-Search Information and witness to the case, had authorisation data and claimed that he was completely unaware of the abuse of power and that his subordinate probably peeped at the authorisation data while he was working with PARSIV.

Initially, the first instance court handed down an extremely clement decision: the two culprits were fined 20,000 and 10,000 rubles (approximately 219 USD and 173 GBP), respectively, and criminal prosecution against them was ceased after the purported reconciliation between the parties initiated by the motion of the investigator. Eventually, Moscow City Court, as an appellate court, overturned this decision and remanded it for trial. However, the trial court again restated the decision. Nevertheless, this case demonstrates that random images can be uploaded and illegally used without consent of the subject and that personal data can be easily leaked and sold in the hidden economy.

Another case worth mentioning relates to the admissibility of facial recognition results as evidence in criminal court proceedings. In February 2023, Alexander Tsvetkov, a 50-year-old hydrologist, was arrested on suspicion of several murders committed back in 2002. The cause of his arrest was that his face, after being captured on video camera, matched a photo of a murderer with 55% probability. He was accused of four murders and taken into custody, despite having an alibi and numerous witnesses testifying for him. He was released from custody only in December 2023 and murder charges against him were dropped only in February 2024.

This case raised the issue of the admissibility and reliability of the use of facial recognition results as evidence in court. The essence of the problem is the absence of a definite rule in the law as to what minimum value of accuracy of results of a facial recognition system is necessary for its use as evidence in a trial. According to the analysis of administrative trials conducted by the interviewed expert, there are no consistent rules developed by judicial practice.

Apart from the facial recognition spreading in large cities, by the end of 2022 when the Unified Biometrics System Law came into force, the government had become an exclusive controller of biometric personal data. Two types of biometric personal data should be stored exclusively in the UBS: facial image and voice. According to Article 15 of the Law, the processing of these two types of biometric personal data is explicitly prohibited outside of the UBS. All the institutions and entities should have transferred biometric personal data they had previously collected in the course of their business operations. Moreover, with the enactment of the Unified Biometrics System Law, the use of biometrics, or to be more exact the use of vectors, became a paid service provided by the government to private entities and sole professionals.

In general, Article 3, parts 15 and 16 of the Unified Biometrics System Law provides such recourse mechanisms as rights to withdraw consent to process biometrics, and to restrict processing of or to erase biometrics and its vectors. However, the establishment of the UBS represents a trend towards further centralisation of personal data processing, and law enforcement authorities have access to the UBS system either through separate IT systems or ESIA, Unified System for Identification and Authentication (Article 14, part 2) or through direct request for information, from which the operator of the UBS is not exempt.

Currently, there is no publicly available evidence of when the UBS was used as a surveillance tool by itself; however, we conjecture that the UBS is just one piece of the whole state surveillance puzzle that complements the arsenal of surveillance instruments available to the government. Our assumptions are that the UBS database can be used later as a source of reference images for facial recognition technology because the UBS itself was designed as a central database that any entity or institution can use as a source of biometrics, namely the so-called biometric vectors, subject to contract with the operator of the UBS. Moreover, there are no legal exemptions that restrict the access of law enforcement bodies. On the contrary, the laws regulating such access, which were mentioned earlier, are quite broad in their scope. The only hindrance to use it not as a vector database but as a database of original biometrics is the scarcity of biometrics data stored in it. The reason is that people are not eager to provide their biometric personal data. Even those who previously gave consent to banking institutions and whose data are subject to transfer to the UBS, resort quite often to their opt-out right provided by the Unified Biometrics System Law.

In September 2023, the Digital Ministry claimed that less than 1% of the entire Russian population had opted out of having their biometrics transferred to the Unified Biometrics System. However, Forbes reported that after fraudulent calls about the impossibility of withdrawing consent to transfer biometrics in the future, the number of people who contacted local state service centres and decided to opt out doubled.

Additionally, we would like to highlight future trends regarding the use of facial recognition:

1. **Further expansion of facial recognition in Moscow city.**

   The newly adopted budget of the city for 2024 has doubled expenses on the federal Safe City Program, which partially includes procurement of video cameras.

2. **The deployment of similar systems in other Russian cities** and (or) development of those which were installed before but are still underfunded. In December 2023, the local authorities of Saint Petersburg reported installing approximately 20,000 smart cameras that enable the use of facial recognition. In addition, the Digital Ministry suggested the

development of a nation-wide centralised IT platform for the storage and processing of video surveillance data. Finally, the Ministry of Transport postponed to 2025 and consecutive years the deployment of surveillance in transportation, including not only airports, but undergrounds and other means of public transportation across the country.

3. **The extension of facial recognition and its deployment in public buildings, such as public schools.**

   Currently, at least one private school in the Moscow region implemented a facial recognition solution developed by VisionLabs, an affiliate of Sberbank. In 2021, NtechLab whose solutions support the Moscow facial recognition system, tested facial recognition in schools across different parts of Russia. In 2023, another vendor, Inoface, a Skolkovo resident, installed facial recognition in seven public schools in several cities of Tatarstan.

Despite low image quality standards and the absence of any parliamentary or judicial oversight, facial recognition results serve as evidence in court, a tool for political repression, and are sold on illegal markets.

At the same time, despite the many risks to human rights (which are considered as unacceptable risks under the new European AI law), Moscow authorities continue to report tens of thousands of cases of catching fugitive criminals and an incredible increase in crime clearance every year. However, the results of studies by independent experts indicate that facial recognition is ineffective in preventing crime and catching criminals. Judging by the available data, in Moscow the clearance rate of serious crimes is below the national average (the leaders are the Bryansk and Tambov regions, where there are no recognition systems). A study by the Collective Action Center shows a slight increase in clearance rates after 2020, but the lack of data on crime and questions about the quality of statistics do not allow us to draw a definite conclusion.

The March 2024 terrorist attack at Moscow's Crocus City Hall, which killed at least 145 people and injured 551 others, has brought Russian society back to the debate over the necessity and effectiveness of some 300,000 cameras in the capital with facial recognition systems which have failed to identify or help catch heavily armed men.

Facial recognition and international law

In 2023, the ECtHR voted unanimously in its judgment Glukhin v. Russia that the use of real-time facial recognition technology without the application of appropriate legally defined procedural guarantees and oversight mechanisms constitutes a violation of the right to privacy, guaranteed by Article 8 of the European Convention on Human Rights of 1950.

On 23 August 2019, the applicant, Nikolay Sergeyevich Glukhin, a Russian national, travelled on the Moscow Metro with a life-size cardboard figure of Konstantin Kotov, a protester whose case had caused a public outcry and had attracted widespread attention in the media. Glukhin held a banner that said: “You must be joking. I’m Konstantin Kotov. I am threatened with up to five years under [Article] 212.1 [of the Criminal Code] for peaceful protests.” During routine monitoring of the internet, the police discovered photographs and a video of Glukhin’s participation in a demonstration in the subway which had been uploaded on a public social media site. Glukhin suspected then that facial recognition technology could be used against him in order to identify him in screenshots of the social media site and in footage collected from CCTV surveillance cameras installed in the stations of the Moscow Metro through which he had transited on 23 August 2019. Several days later, he was arrested after real-time facial recognition technology was allegedly used to locate him while he was travelling in the underground.

Glukhin was subsequently convicted in administrative-offence proceedings for failure to notify the authorities of his solo demonstration using a “quickly (de)assembled object”. He was fined 20,000 rubles (approximately 220 USD, 173 GBP). The screenshots of the social media site and of the video recordings from the CCTV surveillance cameras he passed through on 23 August 2019 were adduced as evidence against him by the police.

On 30 October 2019, the Moscow City Court upheld his conviction on appeal, finding in particular that the peaceful nature of the demonstration he participated in was irrelevant, and that the offence had been discovered and evidence had been collected in accordance with the Police Act; however, it recognised that there had been a breach of his right to privacy as we explain later.

The ECtHR noted that it was difficult for Glukhin to prove his allegation that facial recognition technology had been used in his case. Analysing the issue of the presence and proportionality of interference in the applicant's right, the ECtHR indicated that the legislation of the respondent state, in particular the provisions of the Personal Data Law in force at the time of the events, namely Article 11(2), paragraph 2, was formulated too broadly and did not contain any restrictions on the nature of situations that might lead to the use of facial recognition technology, foreseeable targets, categories of people who might be targeted, or regarding processing confidential personal data. Moreover, the government did not refer to any procedural safeguards, supervisory controls, or available remedies that would accompany the use of facial recognition technology in Russia. That is, national legislation did not even provide for recording of official documents/databases or notifying a person/public about the use of facial recognition technology.

There was, however, no other explanation for the police having identified him so rapidly after the protest. Nor had the government explicitly denied the use of facial recognition technology or clarified how Glukhin had been identified. The ECtHR also took note of public information available regarding numerous cases involving the use of facial recognition technology to identify participants in protests in Russia. It therefore found that the processing of Glukhin's personal data in the administrative-offence proceedings against him – including the use of facial recognition technology to identify and later locate and arrest him – had interfered with his right to respect for his private life.

On the one hand, that interference had a legal basis in the domestic law, as it was stipulated in the promulgated, publicly available legal acts, namely in the Code of Administrative Offences and the Federal Law "On Police". Both laws empower the police to investigate administrative offences and to collect evidence, including evidence containing personal data. In other words, the aim of the interference with Glukhin's rights had been legitimate: to prevent an administrative offence. On the other hand, the ECtHR noted the lack of detailed rules in the domestic law governing

the scope and application of measures involving the use of facial recognition technology, as well as the absence of strong safeguards against the risk of abuse and arbitrariness. The measures taken against Glukhin were particularly intrusive in the face of what had been a peaceful protest, which had not presented any danger to the public or transport safety. It had in fact only led to his prosecution for a minor offence. The processing of the applicant's biometric personal data using facial recognition technology in the framework of administrative-offence proceedings – first, to identify him from the photographs and the video published on the internet, and second, to locate and arrest him while he was travelling on the Moscow Metro – had not therefore corresponded to "a pressing social need" and could not be regarded as "necessary in a democratic society".

The ECtHR considered the measures taken against the applicant "particularly intrusive" because they related to real-time facial recognition technology. The processed personal data contained information about the applicant's participation in a peaceful protest and therefore revealed his political views. Accordingly, they belonged to special categories of confidential data requiring an increased level of protection. The Court also stated that the use of such particularly intrusive technology to identify and arrest participants in peaceful protests could have a negative impact on the rights to freedom of expression and assembly.

In these circumstances, the Court concluded that the use of facial recognition technology to identify the applicant did not respond to a "pressing social need" and is incompatible with the ideals and values of a democratic society governed by the rule of law, which the European Convention is intended to promote and promote.

Afterword: dark surveillance in Russia, deanonymization, profiling and hacking

In this part of our research, we will discuss matters that are worthy of further research. However, the main issue is that the use of profiling and hacking defy comprehensive analysis. The reasons are the dearth of specialised regulations and official documents detailing these two practices. Moreover, there are a lot of oral reporting and anecdotes surrounding them, but there is very little publicly available evidence. These have mostly been reported by insiders and experts. Here, we outline the information which was provided by these experts.

Profiling

Profiling exists in certain aspects of official law enforcement activities, namely as part of the operational-search activities. The so-called operational case, a confidential case opened and conducted by the relevant law enforcement agencies empowered to conduct operational-search activities, falls into common understanding of profiling. However, an interviewed expert drew our attention to the hidden economy of data and certain underhand practices of information intermediaries.

The current landscape can be briefly described as consisting of the following actors. Different software solutions designed specifically for information analytics or Open Source Intelligence.

- For example, Medialogia, a software solution aimed at social media and online mass media monitoring, can be used as a tool for profiling online activity of internet users.
- The autonomous non-profit organization “Dialogue“ (ANO “Dialogue”), an all-Russian Government interagency centre of competence in the field of internet communications and an operator of digital dialogue between the government and society, that helps local authorities to monitor social activity and provides public relation services to them.
- Social Data Hub, which provided its services and gathered information from social networks and application profiles both for the private entities (eg banks) and the government.

Some information has also been brought to our attention about governmental IT solutions, eg Oculus and Vepr (in Russian: Aper/Wild Boar) developed by Roskomnadzor’s subordinate structure, the General Radio and Frequency Center (GRFC). According to the official position, Oculus is designed “to search prohibited content and detect infraction of [relevant] laws on images and videos”. Vepr is tasked

with the “detection of potential strain points in the net, capable of growing into an information threat”. An interviewed expert explained that the latter is responsible for monitoring the most active citizens on the web. Noteworthy is that Roskomnadzor conducts profiling against the political and civil society activists, as revealed in a leak of data from the GRFC (also known as #RussianCensorFiles). For example, there was a list of more than 800 people who are eligible to be declared as foreign agents, of which only 139 were then declared as foreign agents.

There is also unregulated parsing software that extracts online information, quite often protected by the law, and later redistributes it via Telegram bots. The most notorious example was, and quite probably still is, the Eye of God. It was even popular among the police officers from different departments and units because it was far more convenient than their systems and did not require any administrative rigmarole. Moreover, it was revealed to us by a source that developers of such online services quite often provide exclusive access for law enforcement agents.

In 2020, the Ministry of Internal Affairs proposed to consider the possibility of creating a mobile application, the installation of which would be mandatory for all migrant workers arriving in Russia. This proposal is included in the forecast of the development of the migration situation, compiled by experts of the department. As part of the experiment, the Ministry of Internal Affairs proposed to consider the development and formation of a digital profile of a migrant, reflecting the so-called “social trust rating” which should contain full information on the migrant’s social and legal status, biometric data, health information, and criminal record or lack thereof. The idea of such a profile is contained in the Concept of Migration Policy, which the government approved in January 2024.

After the terrorist attack in Crocus City Hall on 22 March 2024, the idea was returned to. Sergei Neverov, vice-speaker of the State Duma, announced that the decision to create such a profile had been agreed with the Prime Minister, and the system will be implemented by the end of 2024. With the help of the digital profile, the Ministry of Internal Affairs will be able to establish where a migrant moves, where and with whom they live, when their permit documents expire, what job they take, and what job they leave.

Deanonymization

In order to be able to identify internet users and punish them for their words, the state aims to carry out digital passportisation of Russian society and deanonymisation of internet users. These goals are not hidden.

Thus, according to the Strategy for the Development of the Information Society until 2030, approved by the Decree of the President of the Russian Federation (paragraph 34e), in order to ensure the functioning of social, economic, and governance systems using the Russian segment of the internet, the Russian authorities need to create new mechanisms of stakeholder partnership and a system of trust that excludes anonymity, irresponsibility and impunity of offenders on the internet.

As can be seen, anonymity is listed comma-separated with irresponsibility and impunity and is seen as a "bug of the internet" rather than its "feature".

In March 2023, as a result of a journalistic investigation, it became known that Rostec had learned how to determine the owners of anonymous Telegram channels and was going to provide this service to the Russian Ministry of Interior Affairs and FSB. According to the developers, the program complex called "Hunter" is able to establish the accounts of administrators and owners of Telegram channels with the help of its own neural network. The personalities of channel administrators are identified by cell phone number, geolocation data, and IP address. In addition, according to the technical description of the program, "Hunter" investigates various sources of open data: social networks, blogs, forums, messengers, bulletin boards, cryptocurrency blockchains, darknet resources, and state automated services.

One year later, there was another investigation by journalist Andrei Zakharov, after which it became known that the Ministry of Interior Affairs had already

purchased in three Russian regions the Insider system as part of the Laplace Demon software for tracking groups, accounts, and chats in VK and deanonymising Telegram users.

Hacking

The legal grounds for hacking are established by the Law "On Operational-Search Activities". An interviewed expert noted that quite often the agents do not have access to the device of the person of interest themselves after its seizure in the course of investigatory activities, but they get help from "black hat hackers" who cooperate, usually involuntary, in exchange for connivance for their crimes.

However, there is no publicly available credible information about successful remote access to users' devices. A reason why this practice of phone seizure for hacking purposes is reported to be popular is because it goes unreported. The expert said that the exact tools in current use are not well-known, but he mentioned that some time ago Elcomsoft and Cellebrite were procured and allegedly used by the government.

And despite the case of Galina Timchenko, publisher and co-founder of Russia's leading independent media outlet Meduza, whose cell phone was infected with the Pegasus spyware, it is still unknown who was behind the attack. There is currently no information about the sale of Pegasus installations to Russia by NSO Group.

To conclude, we believe that these two aspects, profiling and hacking, merit further research with a focus on fact finding and verification. Such research might contribute to better understanding of the realities of the use of profiling and social monitoring, as well as threats associated with the use of hacking against activists, business people, and politicians.

Conclusive arguments

To summarise, Russian state surveillance has the following characteristics:

- Targets indiscriminately citizens, as well as foreigners, including working migrants.
- Exists in the context of ongoing attempts to passport every internet user and deanonymise users of social networks, including with the use of technological solutions.
- Infringes on the principle of proportionality due to the use of unaccountable surveillance over internet communications, as specific approaches or criteria are classified and surveillance can be used indiscriminately.
- Lacks effective means of legal redress for those whose right to privacy has been breached by the government officials.
- Relies on technical infrastructure integrated into the networks and service providers as agents of state surveillance which enables mass surveillance over users.
- Its legal regulation for the use of biometric personal data for surveillance purposes is non-existent, which blurs the boundaries between online and offline surveillance, and makes the system unaccountable and liable to abuse and corruption.
- The lawmakers constantly use open-ended goals and relevant wording when they draft laws, thus ensuring the wide discretion for law enforcement, which consequently leads to abuse of power.
- There is a patent strategy of the government disguising the use of facial recognition technology and controversial practices behind “legal experiments”, extremely vague wording, or behind restricted access to internal documents subject to confidentiality and other protective measures.

Team

RKS Global

info@rks.global ▪ rks.global/en