By the end of 2022, Russia had adopted a new law regulating the rules for the collection, storage and usage of biometric data — i.e. unique biological and physiological information about a person that enables unambiguous identification. This includes fingerprints, pictures of the face and iris, voice samples, and the pattern of veins on the palm and fingers. So far, about 70 million Russians — roughly half of the population — have submitted their biometric information to various organizations and institutions, mostly banks. The authorities claim the new law is intended to protect this data and put an end to «biometric anarchy» in the country. However, in reality the law establishes the state's monopoly on the use of biometrics and gives the FSB and
other security agencies free access to biometrical data. It should be noted that these are the very agencies which have repeatedly been found to use the new technology for political repression.

A month after the law was signed, it turned out the Russian authorities had already planned several projects to control citizens with the use of biometrics. They intend to install facial recognition cameras at the state border, to implement a system that will search for the faces of opposition activists in online videos, and to use facial recognition technology on surveillance cameras in Moscow to find conscripts who evade military registration and enlistment offices. Against this backdrop, Russian society, already terrified of political repression unprecedented in the history of modern Russia, is increasingly being vocal about the dangers of total surveillance performed by the «Big Brother.» Critics of the biometrics law, including — quite unexpectedly, — some MPs, have referred to the surveillance system as a «digital concentration camp» or «digital GULAG.»

**Russian algorithms topping global rankings**

Biometrics is one of the few kinds of technology in which Russia has made a visible breakthrough in the last few years. At least a dozen major biometric companies are now operating on the Russian market, and the algorithms of half of them have been featured regularly in the top ranks of world biometric competitions over the past eight years, in particular the biometric technology rating issued by the National Institute of Standards and Technology (NIST) at the US Department of Commerce. Technologies devised by these companies can recognize people's faces and voices, detect their silhouettes in a crowd and recognize their actions, capture and verify fingerprints, as well as detect and read colors, models and license plates of cars in traffic.

The state couldn't help but notice such a breakthrough — this explains why in the last five years government agencies have bought up all of Russia's top biometric companies. The NtechLab, the most successful Russian company in the field of biometrics, is now co-owned by two state-owned companies: Rostec Industrial Conglomerate Corporation and Russian Direct Investment Fund. Today, NtechLab is the government's main contractor for its projects related to the identification of citizens. Sberbank first acquired a large stake in VisionLabs, and then its example was followed by oligarch Vladimir Evtushenkov's AFK Sistema. VisionLabs is now the key contractor working on the FacePay project commissioned by the Moscow Mayor's office. The project will enable passengers to pay their metro fares through the system of face recognition. Gazprombank was the first main owner of the Speech Technology Center, which specializes in voice recognition, and later own this role was taken over by Sberbank. The venture fund of the National Technological Initiative made an investment into 3Divi, a project created in 2014 on the personal instruction of Vladimir Putin to develop technology in the country.

The big interest in biometrics in Russia dates back to the late 2015, when an algorithm developed by an obscure domestic startup NtechLab suddenly found itself at the top of the world facial recognition championship The MegaFace Benchmark organized by the University of Washington, surpassing by some parameters even the algorithm FaceNet designed Google. Until that moment, the use of biometrics in Russia was mostly limited to dactyloscopy, which was employed mainly in forensics, border control and access control systems in closed facilities.

A couple of months after their triumph at the competition, NtechLab launched a public service called Findface so as to demonstrate its capabilities to the public. It was a well-intentioned idea. Its creators presented it as a sort of dating service, which allows you to upload a photograph of any person to the portal (for example, a photo taken on the subway) and then find this person's profile and all the publicly available personal data in the most popular social network
in Russia, Vkontakte (VK), so as to ultimately meet the charming stranger.

However, Findface immediately demonstrated the abuses that can result from a careless attitude toward biometrics. Users of the popular Russian anonymous forum 2ch launched a campaign using Findface to «unmask» or identify porn actresses: they used Findface to find their accounts on VKontakte, sent insulting messages to their inboxes and sent pornographic videos featuring these actresses to everyone on this person's friend list.

As a result, Russian Internet users began using Findface en masse for deanonymization, harassment and surveillance. Its founders shut the service down two years after its launch, as Findface began to pose a serious threat to the reputation of NtechLab, which by that time had become a big player in the biometrics market, with investments from Roman Abramovich’s ImpulseVC Foundation and the Russian defense holding company RosTech. NtechLab is currently the key partner of the Russian authorities in the sphere of biometric technology. Its facial recognition technology is used in CCTV cameras throughout the city of Moscow and in the Moscow subway: the program tracks people’s movements, identifies faces in the video stream and compares search results with the Interior Ministry’s databases, allowing it to find wanted persons.

The company’s main shareholders today are the entities of RosTech, the Russian Direct Investment Fund (RDIF) and the fund of businessman Ruben Vardanian. NtechLab founders Alexander Kabakov and Artem Kukharevskiy, who were previously quite satisfied with their cooperation with the Russian authorities, left the company after the onset of the full-fledged invasion of Ukraine citing disagreements with its top management and investors.

The success of NtechLab, which created what by world standards amounted to an advanced algorithm, was clearly not an accident. In the mid-2010s the Russian market saw a real boom in successful projects in the field of biometrics. For several years in a row, domestic companies, such as VisionLabs, Vocord, 3Divi and the Speech Technology Center (SRT), along with NtechLab, have been in the top ratings of biometric technologies devised by NIST. At the heart of their success is the tradition of mathematics teaching, which is still strong in Russia and allows it to produce many top-notch developers and mathematicians. In addition, biometrics itself was becoming a very «fashionable» technology around the world: in the West, it began to be actively used in consumer electronics, the financial sector, and retail.

Creating a Unified Biometric System

According to the Ministry of Digital Development of Russia, by the end of 2022, biometric data had been sourced from 70 million Russians, or half of the country’s population. This was done primarily by large Russian banks: the banks were the first in Russia to pay attention to the growing market of biometrics and the success of domestic developers of mrecognition algorithms.

The pioneer among banks was the state-owned Sberbank, whose customer base currently exceeds 100 million people. Sberbank announced widespread introduction of biometrics in May 2016. Bank branch employees started to collect voice samples and face photos from their customers, promising to open accounts, give loans, or verify remote electronic transfers in the future. Sberbank was followed by other credit institutions of the country, and as a result, biometrics has gradually become very «fashionable» with financial institutions.

It was then that the state regulator of the financial sector, the Central Bank, joined the race. In early 2017, it announced the creation of the Unified Biometric System (UBS) — a database for
the centralized storage of voice samples and facial images of bank customers. According to the concept, any person who submitted his or her biometric information to one of the banks could remotely open an account and receive services at all other financial institutions connected to the system. The Central Bank made it obligatory for all credit institutions in the country to connect their branches to the UBS by the end of 2021.

The banks had no choice but to comply. As a result, all major financial institutions in the country began to massively source and accumulate voice samples and facial images from private citizens. The official state position stipulated that biometric data collection was voluntary, but in practice the collection of such data was accompanied by aggressive marketing and «occasional overzealousness.» Every now and then reports surfaced of customers who went to some branches of banks and were denied services or were not issued bank cards unless they agreed to provide biometric data.

By the end of 2022, the largest banks in the country had collected biometrics from half of the country's the population, yet it turned out that more than 90% of this data was accumulated not in the UBS, but in the banks’ own databases. The reasons for this were many, and they were both legal and technical. The key factor behind the banks' not sharing the accumulated data with the USB was a legal loophole: the law obliged the banks to join the UBS, but did not make it compulsory for them to transfer their data there. Considering that for each request from the UBS the bank has to pay 200 rubles (2,30 euro), financial institutions decided it was more profitable in the long run to create their own biometric databases.

The Kremlin, however, was not happy about this development.

**Biometrics under FSB control**

In December 2022, Vladimir Putin signed a new law on biometrics postulating that the biometric data of Russians should now only be stored within the UBS. Storage and processing of biometric data outside of this system is now prohibited: all banks and other commercial companies will have to transfer all the biometric data to the UBS and purge this data on their own servers.

An important nuance of this law is that it grants full control over the UBS to the Federal Security Service (FSB). The FSB will be in charge of setting the key operating conditions and parameters for the UBS. For instance, it will decide which agency will be the system's operator, how biometric data should be submitted via smartphones, and how to «monitor compliance with organizational and technical measures for ensuring the security of biometric data.» The FSB and other security agencies will have a powerful mandate enabling it to obtain any person’s biometric data from the UBS if they so desire.

The new law clearly states that the UBS operator must provide biometric data to the FSB and the Ministry of Internal Affairs, if these departments submit a valid request. It is obvious that the consolidation of all biometric data into one state-controlled and state-run database will greatly facilitate access to it for the law enforcement agencies.

The absence of democratic mechanisms of control over the use of such sensitive information has already opened up a huge space for abuse by the state apparatuses. Russia is one of the global leaders in the use of video surveillance cameras. In Moscow, surveillance cameras equipped with facial recognition systems are used en masse on the streets and in the subway, a system that has already enabled security forces to track activists and protesters. Thus, after the start of mobilization in Russia in September 2022, police used CCTV facial recognition systems in the subway to track citizens who had previously participated in protests and detain them. Now the
state has gone even further and plans to use cameras to identify potential conscripts on the streets of Moscow who evade going to the military registration office.

Among residents of large Russian cities, such use of biometrics has already caused discontent. In 2019, human rights activist Alyona Popova sued the Moscow mayor's office, stressing that the authorities were processing citizens' biometric data in violation of the law on personal data protection and the Constitution. A year later, she and her colleague Vladimir Milov filed an appeal with the European Court of Human Rights, complaining about the authorities' use of facial recognition technology during the protests that followed September 2019 Moscow City Duma elections.

The new law on biometrics caused even more dissatisfaction in society, even in the pro-government circles. The law sparked local protests in some regions, which is a rare occurrence in modern Russia, since against the backdrop of the war against Ukraine, law-enforcement agencies have been cracking down on any protest rally in the country. Representatives of the Russian Orthodox Church, led by Patriarch Kirill, who usually refrains from criticizing any policies proposed by the current government, also spoke out against the law. The patriarch said that the church advocates the fundamental right of citizens to refuse biometric identification and asked not to discriminate against people who have made such a choice. However, it was the MPs representing the Communist Party in the Duma who advanced the harshest criticism of them all, calling the new law on biometrics «antinational» and warning that a «digital concentration camp» is currently being built in the country.

Russian authorities are now preparing to install CCTV facial recognition systems at land borders. The problem of illegal state border crossing is very acute in Russia. Over the past year several oppositional activists and people who were prosecuted for political reasons left the country illegally.

Another important aspect of this project is the introduction of what essentially amounts to compulsory collection of personal biometric data from all citizens crossing the Russian border. You simply won't be able to cross the border and leave the country unless you submit your biometric face print.

The authorities are also planning to make extensive use of biometrics on the Internet. The federal censorship agency Roskomnadzor has recently launched Oculus, a system based on artificial intelligence that will search for online photos and videos of insults against the authorities, as well as recognize the faces of opposition activists.

**Technology as a tool of repression**

Biometrics is yet another technology that is turning into a weapon for political repression when used by the Russian regime. The situation is compounded by the fact that because of the war in Ukraine, the Putin regime has begun to put new pressure on those who disagree with its policies, and biometrics could be of huge assistance in their effort to track and prosecute dissident-minded citizens.

Russia is now consistently moving toward the introduction of biometric control in all public places in large cities, at important infrastructure facilities and on the Internet. In response, an active segment of the population is increasingly speaking out about the dangers of total state surveillance of the population, which violates the rights of ordinary people to privacy and confidentiality and contradicts the Constitution.
A separate reason for speculation about surveillance is the fact that the active spread of biometrics in the country is presented as part of the state project «Digital Profile of the Citizen», which is designed to consolidate all available information about citizens in a single database. Some members of the Human Rights Council oppose this initiative, noting that its concept is similar to the social rating system being tested in some Chinese provinces and leads to discrimination and abuse of citizens.

Another point of public concern in connection with the large-scale collection of biometrics into a single state system is the vulnerability of such databases in Russia to leaks and hacks. Various personal data of Russian citizens are freely traded on the darknet. It was thanks to this, for example, that a couple of years ago investigative journalists managed to make public the real names and documents of the GRU officers who attempted a poisoning of Sergei Skripal in the UK. Politician Alexei Navalny, too, managed to find the names of his FSB poisoners on the darknet. Since even the data of employees of special services is not secure from leaks, the serious protection of information about ordinary citizens is out of the question. The leakage of biometric information can create a huge wave of fraud in the country, taking into account that banks and state services are increasingly turning to biometric identification in their operation when providing services to citizens. A single database with such sensitive information as biometric prints would be an obvious target for hackers, and the Russian government has not disclosed any clear plan as to how it plans to protect it.