INTERSECTION
RUSSIA / EUROPE / WORLD

• Author: Damir Gainutdinov

Surveillance in Russia

The Federal Security Service of the Russian Federation — the FSB — has demanded that Telegram, a popular encrypted messenger service, hand over its "universal key," which would allow the FSB to access all users' private conversations. The FSB wanted this sent over to a general unprotected address — fsb@fsb.ru — which, on the internet, is the equivalent of leaving it at the reception. Telegram, known for its high data-security standards, was fined 800,000 roubles for refusing to comply with this absurd demand. Aleksandr Plyushchev, a journalist with the radio channel Echo of Moscow, filed a complaint with the Meshchanskiy district court in Moscow that his confidential correspondence with sources had been violated; instead of answering him, the court published Plyushchev's home address on its website. For some time, the court personnel were claiming this was routine procedure; it turned out that one single judge had openly posted about ten other home addresses.

Both instances say a great deal about the Russian state's widening attempts to keep watch on its citizens. When questioning and searching people, Moscow police have started asking detainees to hand over their personal mobile phones, and they browse personal files with impunity. One of the world's biggest video surveillance systems went into operation in Moscow this autumn. It combines almost 130,000 video cameras, 3,000 of which have sophisticated facial-recognition capabilities. Who will use them – and for what purpose – is a big question, considering the state's complete inability and unwillingness to protect citizens' personal data.

One may remember incidents when car owners' personal data were published on the Internet; or when a branch of the Russian pension fund sent out almost 18,000 people's personal data in an open mass email. Another example was when the investigative committee refused to look into a case at Moscow's Savelovskiy market, where a local MIA information centre database was on sale, containing addresses, medical diagnoses, and even conviction details of 400,000 Moscow residents.

Widening surveillance, leaky storage

This means that the Russian authorities are amassing various data (including extremely sensitive information) on Russian citizens and foreign guests, but storing it in a way that cannot guarantee its safety, even in everyday circumstances. Information is gathered on the seemingly noble pretext of fighting terrorism, extremism, and guaranteeing public safety. In practice, it turns into selective monitoring of independent civic activists, journalists and members of the opposition – tracking their movements inside the country and when leaving it, eavesdropping on their conversations, and intercepting their messages and emails, mounting outdoor and discreet surveillance, as well as gathering and processing biometric information (fingerprints, DNA, photographs, etc.).

This is only for formally legal types of investigation, not involving hacking into email or social media accounts, etc. However, a new 2017 analysis has revealed that various state authorities are now scrutinising not only "unreliable" citizens, but also football fans, their own law-enforcement officers, holders of real estate, bank accounts and companies abroad, not to mention all Russians resident abroad, be it temporarily or permanently.

Who keeps watch over surveillance procedures?

The problem is, there is basically no control over those in charge of surveillance. Unlike a number of other spy agencies around the world, accountability procedures are not in the offing. According to Agora International's analysis of the open statistics provided by the Russian Supreme Court's Judicial Department, courts *automatically* approve of encroachments on the privacy of individuals. In the last decade, Russian courts acceded to 98% of law-enforcement agents' requests which violate rights to private correspondence and communication.

As a result, all Russian citizens, even those with no connections to activism or opposition whatsoever, live under a constant threat of someone accessing their private data through mobile phones, the Internet, or various video surveillance systems installed in public places – from stadiums to trade centres – which the authorities are happy to advertise. Citizens are under surveillance during contacts (even accidental ones) with any law-enforcers. Their use of banking services, public and private transport, job applications to a whole range of organisations, foreign travel plans, and applications for weapon licences are all closely monitored. The authorities also keep various registers and databases on certain categories of persons on watch lists. They also perform administrative supervision, and keep "black lists" based on a logic of their own. Whenever it becomes clear that controlling everything is impossible, the state delegates its surveillance authority to non-governmental bodies, such as Internet and telecommunications providers, shipping companies, and banks. All of them are dependent on the authorities (which provide access to the market or state budgetary funds) and, of course, they hold all the necessary information about ordinary people – their clients. Neither the right to privacy nor any presumption of innocence are respected. In a report our organisation published recently, we highlight that the number of requests for wiretap authorisations has risen three times in ten years, since 2007.

Most interestingly, all the legal conditions for legitimate gathering of information on almost all Russian citizens are effectively in place. However, we registered numerous examples of the state's inability to competently gather, safely store and efficiently analyse the collected data. The implementation of the infamous "Yarovaya law" concerning online surveillance will cost from 130 billion to 10 trillion roubles. The authorities will require telecommunication and Internet service providers to store the content of voice calls, text messages, photographs, videos and sounds for half a year, and to provide the FSB with all their users' decrypted correspondence. Where will the funds for this come from? The answer: from our own pockets, through steep price rises for these services, and the additional burden on placed on private business. After the minister of communications, Nikolay Nikiforov, recently submitted the draft of the Russian government resolution on implementing the "Yarovaya package" for its final approval, lawyers from RosKomSvoboda and

the Digital Rights Centre wrote him a letter, underlining the absurdity of the situation, and stating that the "Yarovaya package" cannot be implemented in full. The lawyers emphasised that the subordinate legal acts drafted by the ministry of communications are in contravention of penal and procedural legislation. They also noted that the period for which users' conversations, text messages, and all transferred files (photo, video, sound) can be stored should not exceed 24 hours, and the currently requested six-month term should only be possible for certain individuals, and strictly by court order.

Currently, people either accept blanket surveillance as a necessary evil, or find ways to protect their personal lives, and keep away from the eyes of law enforcement. At the same time, we should not be surprised if the authorities see people's wish to protect their privacy as a sign they have "something to hide."

*Damir Gaynutdinov is a co-author of the independent report by the Agora International Human Rights group "Russia Under Surveillance 2017".

Tags
media freedom
censorship
Media
Category
Politics