Surveillance pandemic

The global health crisis caused by the coronavirus pandemic has served as a pretext for a major expansion of surveillance in a substantial part of the world. Citizens of authoritarian states are the most vulnerable. In Russia, the introduction of quarantine became a catalyst for the development of all kinds of tracking methods, first and foremost digital technologies. This was only limited by the financial capacities of regional authorities, to whom the key powers to fight the pandemic have been delegated. Wealthy regions have been given carte blanche to exercise full control over residents' movement by any available means.

We counted six separate technologies for collecting and verifying information about citizens' private lives, which, taken together, immerse us into a "brave new world" of total surveillance: centralised collection of information about citizens arriving in the country, region or populated area; a system of digital or analogue passes, making it possible to limit both means of transport and purposes of travel, as well as differentiate citizens according to the rights afforded to them during quarantine; video surveillance, including facial recognition functions; tracking citizens' location using geolocation data from mobile devices and tracking apps; expansion of surveillance capabilities by means of delegating police functions to private entities and representatives of other departments.

In future "emergencies", that can be declared under any circumstances – from a new epidemic or technogenic accident to mass protests – the experience and resources accumulated during quarantine will allow the rapid deployment of close surveillance, and for differentiation of citizens according to the amount of rights and freedoms to which they are entitled under the regime. Moreover, it turns out that, in order to do this, the

authorities don't even need to officially declare an emergency situation or state of emergency.

There are essentially no laws in Russia regulating the extent of interference into citizens' private lives with the aid of digital technologies. The existing provisions of the Constitution and norms of relevant branches of the legislation are undermined by law enforcement practices and the absolute support given by the Russian courts to the executive and law enforcement authorities.

Furthermore, it has become clear that a number of regions and departments intend to keep some of the tested technologies in "peacetime". For example, the authorities of Belgorod Oblast requested, on their own initiative, for the region to be included in a trial of a tracking application developed by Ministry of Digital Development, Communications and Mass Media (Minkomsvyaz), citing the need to prepare for future emergencies.

In addition, it has been reported in the media that the Russian Ministry of Internal Affairs is considering using tracking apps and introducing a "social trust rating" for all migrants entering the country.

It is safe to assume that apps tracking geolocation will be used as a means of monitoring compliance with restrictive measures, such as house arrest, administrative supervision etc.

The development of coronavirus surveillance methods has resulted in the expansion of the use of other forms of technology and practices, which are not directly related to the pandemic. For example, the Ministry of Internal Affairs, Federal Security Service (FSB) and Minkomsvyaz have already prepared a bill that would make it mandatory for communication service providers to store information on all text and voice messages, video and audio recordings, images, and any other communications received, transmitted or processed for all owners of telecommunication networks and Internet exchange points for a period of three years.

Moscow's "Big Brother"

In contrast with the overwhelming majority of Russian regions, which have limited themselves to individual measures, Moscow has made the most of quarantine, organising large-scale testing of various digital and "analogue" technologies for establishing control over citizens. While, previously, only certain "suspect" categories of citizens were subject to monitoring (extremists, civil activists, football fans, human rights defenders, members of informal associations and subcultures), such tracking now extends to

ordinary citizens, who have been divided into categories according to the amount of rights and opportunities to which they are entitled.

In essence, "pandemic 2020" has become the second pretext, following the FIFA World Cup 2018, for the development and testing in "combat conditions" of technologies intended specifically for mass surveillance. Strictly speaking, Moscow has had many more opportunities and justifications for this compared with other regions: on the one hand, the capital is a leader of digital development, and on the other – it is the largest centre of infection in the country.

By 2020 Moscow was the home of Russia's largest network of street and underground CCTV cameras connected to a facial recognition system. According to the Moscow Department of Information Technologies, the network comprises more than 178 thousand cameras in 102 thousand residential building entrances and 21 thousand courtyards, not including cameras installed in state and municipal buildings and other public places. This network has been used to identify quarantine violators.

The Moscow authorities were among the first to announce the introduction of digital passes, and were able to swiftly launch this system on the basis of the city's portal of public and municipal services. The system tracked movement using data from travel cards and car number plates, while the network of street cameras was used to record violations and issue mass fines for travelling through the city without a pass.

In fact, what we can observe in Moscow is the largest mass surveillance network, coupled with differentiation of citizens according to the amount rights and freedoms to which they are entitled under the quarantine regime. In this respect, the capital's residents can provisionally be divided into four categories.

The privileged. These citizens don't have to self-isolate, are allowed to leave their place of residence, including in order to go to work, are not subject to electronic monitoring and don't have to obtain a digital pass. This group includes employees of governmental organisations and departments, whose presence in the workplace is essential for the running of the organisation, healthcare workers, as well as other citizens identified in the order of the coronavirus Headquarters; employees of law enforcement authorities, Ministry of Emergency Situations, and Rospoterbnadzor (Federal Service for Surveillance on Consumer Rights Protection and Human Wellbeing); volunteers, taxi drivers, construction workers, and employees of essential businesses; military personnel, state and municipal employees, persons

standing in for state and municipal posts, judges, lawyers, notaries, including assistants, journalists, private security guards.

Ordinary citizens. This group includes all citizens who do not fall into the other categories, who have to comply with quarantine and register for a digital pass to leave the house; the number of such passes and their duration are limited.

Persons with restricted rights. This group includes persons arriving from dangerous territories and those living with them, persons older than 65 years, as well as citizens suffering from diseases included in the list approved by the authorities. These citizens must self-isolate and can't leave their place of residence without special grounds for doing so, which requires a digital pass.

The isolated. These are persons who have been diagnosed with COVID-19 or an acute respiratory infection, and those living with them (in accordance with individual orders). They can't leave their place of residence, and are subject to mandatory electronic control using the "Social monitoring" mobile tracking app.

Russia-wide measures

Since the beginning of March 2020, Russia's chief medical officer issued a series of orders aimed at reducing the risk of importation and spread of the new coronavirus infection, according to which the heads of all Russian regions must ensure that all persons arriving from abroad self-isolate for 14 days from the date of entry into the country, and also organise control over compliance with the quarantine regime, as well as the running of the coronavirus hotline for collecting information on citizens.

The regional authorities have, in turn, transferred these control powers to the municipal level. For example, the governor of Astrakhan Oblast, Igor Babushkin, expressly stated the following at a meeting of the heads of regional authorities: "All citizens who need to self-isolate in connection with coronavirus must be monitored by employees of the internal affairs services. And you also have to know everything about them".

In addition, every person arriving from abroad was obliged to notify the authorities of his or her return to the country, providing a substantial amount of personal information in the process – places and dates of stay abroad, as well as the addresses of registration and residence in Russia.

Some of the regions began introducing such restrictions earlier, however, they often requested less information. For instance, Muscovites were required to report their arrival from countries and territories in which cases of coronavirus had been recorded as far back as 5 March, but, besides contact details, no other information was requested. In St Petersburg, Novgorod Oblast, and a number of other regions, reporting to the Rospotrebnadzor coronavirus hotline initially took the form of a recommendation.

At the same time, the authorities made it clear that, in any case, they know who has crossed the state border, reminding citizens of the administrative and criminal liability entailed by failing to comply with quarantine, which is being monitored by police with the support of the FSB, voluntary people's guards, quasi-public associations, Cossacks, rescuers, and other involved entities. Cases are known of citizens who had returned from abroad, were not questioned at the border and did not report their arrival via the hotline, but nonetheless received phone calls from their local polyclinic, were questioned about their wellbeing, and reminded of the need to self-isolate.

Patients diagnosed with coronavirus and those arriving from abroad have been subjected en masse to epidemiological investigations conducted by employees of Rospotrebnadzor, including surveys at airports and railway stations, as part of which they were required to provide information such as their address, contact telephone number etc. Medical workers visited them at their homes and collected information on persons living with them, their neighbours, co-workers, and close relatives. The possibility of conducting sanitary-epidemiological investigations is provided by Article 42 of the Federal Law "On the Sanitary and Epidemiological Wellbeing of the Population", however, the special legislation does not allow Rospotrebnadzor to collect and process information about citizens' private lives, and does not determine the boundaries of interference into private life at all.

Subsequently, in a number of regions the need to notify the authorities of one's arrival in the territory was extended to all persons crossing the administrative border of a constituent territory of the Russian Federation. In Murmansk Oblast, people were obliged to report the place and dates of their stay in the territories of other Russian regions, and provide their contact details, including the address at which they were self-isolating.

Regional coronavirus hotlines became the first link in the chain of collecting information about citizens under the pretext of fighting the pandemic. The next level was information processing and exchange.

On 31 March the government approved the Temporary Rules for Recording Information to Prevent the Spread of the New Coronavirus Infection, which consolidated the centralised data exchange system. According to this document and the methodological recommendations of the Russian Ministry of Health, when collecting epidemiological anamnesis, information is to be obtained on any trips abroad within 14 days of the onset of first symptoms, as well as close contact over the last 14 days with any persons suspected of infection, or those whose diagnosis has been confirmed by laboratory testing.

The centralised database includes the following information on persons with a confirmed coronavirus diagnosis, those who have been hospitalised with pneumonia, as well as everyone who has had contact with the said persons: surname, first name, patronymic, date of birth, sex, citizenship, address of registration and actual residence, mobile phone number.

Those infected with COVID-19 or hospitalised with pneumonia are required to provide a wide range of medical and epidemiological data: information on medical insurance, any medical examinations and the medical institutions at which they were performed, pregnancy, vaccination, accompanying diagnoses, travel[1], including in the territory of Russia (the document used to purchase tickets, points of departure and arrival, route taken etc.) Furthermore, on the decision of the operational headquarters, the database may be supplemented with any other information deemed necessary by the headquarters. The operator of the database is the Ministry of Health, and it can be accessed by any subordinate institutions of the Ministry of Health, Roszdravnadzor (Federal Service for Surveillance in Healthcare), the Ministry of Internal Affairs, the Federal Medical-Biological Agency, certain "information providers", and "other bodies and (or) organisations on the decision of the operational headquarters". Such decisions are not published or explained.

Additionally, Minkomsvyaz obtains information from mobile phone operators on a person's movement within the country on the basis of billing details and enters this data in the centralised database. This system must be used, in particular for tracing the contacts of patients and infected persons, as well as to send notices requiring citizens to self-isolate.

1 We note that, according to the rules of passenger transportation (air, rail, and intercity bus travel), when purchasing a ticket citizen must show their passport, and passenger information is registered in centralised databases accessible to police. Together with the "Surveillance Control" system, this allows to track the movement by public transport of any persons of interest to the authorities.

In practice, some mobile phone users in Krasnoyarsk and Krasnodarsk territories received messages from the telephone subscriber "MCHS" with the following content: "We strongly encourage you to return home! Refrain from going out for walks! By being on the street, you are putting your life and the lives of others in danger! Leaving home for non-essential purposes is prohibited!" Russian telecommunications company PJSC VimpelCom refused to provide information on the limits and grounds for tracking subscribers' geolocation data, while the Ministry of Emergency Situations and the mobile services company Scartel LLC ignored a lawyer's enquiry.

In Tatarstan, the first version of the portal for obtaining SMS-passes contained the following warning: "If you systematically stray from your home during the course of the day, the system will pick up on this, and measures will be taken". Since there was no requirement to install any special software on mobile devices, the intention was, presumably, to track movement based on data held by mobile phone operators. This warning was later removed from the website.

At the beginning of June, Minkomsvyaz published a draft regulation on exchange of information on the location of citizens who have had contact with COVID-19 patients, determined on the basis of mobile phone operators' data. According to the document, Minkomsvyaz will receive daily information from operators on all of the following subscribers:

- those who are abroad;

- those who have crossed the border of the Russian Federation (for these persons, compliance with self-isolation requirements will be monitored, as well as movement outside the self-isolation zone (from 500 to 2,000 metres) during a 14 day period from the date of crossing of the state border, based on the subscriber's location on the first night of arrival);

- those who have possibly had contact with infected subscribers (on the basis of geolocation data, information on calls and SMS messages).

Minkomsvyaz, the Ministry of Health, the Ministry of Internal Affairs, the Russian Guard, bodies of the executive authorities and regional headquarters would all be able to access the system.

Collection of information directly from citizens, as well as centralised processing of geolocation data, are the only measures that have been adopted nationwide. With regards to everything else, regional authorities have been able to choose their own strategies and methods of tracking, which they have made use of to varying degrees.

"Analogue" and digital passes

The authorities in 23 Russian regions and Sevastopol have introduced some form of so-called "digital passes" - codes made up of letters and numbers, which must be obtained in order to leave the house during the quarantine regime, or to travel on private and/or public transport. In 15 regions, as well as Crimea, "analogue" passes have been introduced (issued, as a rule, by employers to those employees who are allowed to continue working on-site), either as a stand-alone or additional measure. Furthermore, 19 regions have announced that they are ready in principle to introduce digital passes in case of worsening of the epidemiological situation, or in future in the event of an emergency.

Systems for issuing digital passes were developed in an expedited manner, without an independent audit, which certainly had an impact on both quality and security. For example, soon after the release of the corresponding app in Moscow, experts identified a whole range of security breaches – the app obtains access to all information and settings, including establishing connections with bluetooth devices, GPS, camera and calls, turning off sleep mode, viewing network connections; the app transfers the information collected openly, without encryption; for facial recognition, the app uses the Estonian service identix.one, transferring data through servers located outside the Russian Federation; the device's MAC and IMEI individual identifiers are encrypted in the QR-codes generated by the app.

In Moscow, when registering for a digital pass, citizens were required to give the Department of Enterprise, Department of Information Technologies, and a number of other institutions subordinate to the Moscow authorities, permission to process transmitted personal data, which includes transfer to third parties and for advertising purposes for a period of ten years.

Delegation of police functions

The authorities of almost half of the Russian regions have granted extraordinary powers, including the possibility of interference into the private lives of citizens, to a wide range of subjects – from medical personnel and rescuers, to taxi drivers, voluntary people's guards, and members of Cossack societies. This has led, in particular to the implementation of clearly unlawful discriminatory practices against representatives of vulnerable groups.

One of the main measures adopted in Russia to counter the epidemic is self-isolation of citizens and restriction of travel, both between constituent

territories of the Federation, and within populated places. The restrictions depend on both the purpose and means of travel, and sanctions are provided for any violations.

As of 1 April the Federal Code of Administrative Offences was supplemented by norms introducing penalties for failure to carry out anti-epidemic measures during an emergency situation, quarantine, or threat of the spread of dangerous diseases (part 2, Article 6.3), as well as failure to comply with rules of conduct during a high alert regime (Article 20.6.1). Such norms also appeared in some of the regional administrative offences codes.

Following the introduction in the Russian regions of a high alert regime, the territorial headquarters of the Ministry of Internal Affairs received instructions to provide assistance to the executive authorities with the implementation of measures to counter the spread of the new coronavirus infection.

As quarantine and self-isolation requirements for citizens arriving from other constituent territories of the Russian Federation were being introduced in a number of regions, the municipalities, in turn, were instructed to organise the collection and submission to the Ministry of Internal Affairs of information on such citizens.

The main task became identifying citizens arriving in the region, as well as creating conditions for monitoring self-isolation (including photography, surveys, collection of information on actual place of residence and stay), and ensuring compliance with quarantine measures (reasons for leaving the place of residence, possession of a pass).

In at least 38 Russian regions, as well as the territory of the Crimean peninsula, the authorities have involved outside parties in enforcing such control measures – members of veteran and "military and patriotic" organisations, voluntary people's guards, members of local "mobile groups", cadets, officials of municipalities, representatives of the All-Russia People's Front[2], employees of municipal institutions and social organisations in the spheres of culture, sport, and education, employees of fire fighting and rescue centres, sportspeople.

They generally patrolled the streets alongside police officers, limiting themselves to explaining the need for social distancing and self-isolation to citizens. However, cases of more serious restrictions of privacy are known.

2 A political coalition created in 2011 on the initiative of Vladimir Putin.

For example, the Krasnodar authorities reported on the creation of "mobile self-control units for patrolling the streets and public spaces", who "send home those who are violating quarantine or are found to be outside without a reason; those who refuse to go home will face administrative and criminal measures".

In Primorsky Krai the authorities invited a private company to monitor the territory using industrial drones equipped with thermal cameras.

Besides checking documents, Cossack patrol units in, at the very least, the Ryazan and Sverdlovsk regions, have carried out ethnic profiling. In an interview to a state news agency, a representative of a Cossack society maintained that the patrols "look at people of "Chinese ethnicity" and everyone who sneezes, take notice, invite them to come to the polyclinic accompanied by the patrol, but on a voluntary basis". We note that ethnic profiling has been recognised as one of the forms of discrimination prohibited under international law.

In accordance with the law, such functions (excluding clearly unlawful actions), by way of exception from the general rule of protection of private life and freedom of movement, are assigned to the police and the Russian Guard. Quarantine has forced the authorities to significantly broaden the circle of persons (to an indefinite number) who are permitted to question citizens, monitor them, and restrict their freedom of movement, endowing these persons with ambiguous powers.

In addition to collecting epidemiological anamnesis information, in some regions, where cameras and facial recognition systems are used to monitor compliance with quarantine, medical workers have been instructed to enter information about patients, including their surname, name, patronymic, diagnosis, and other medical data, into centralised database systems, and also photograph them – clearly extraordinary powers that are not typical of doctors.

At the same time, while the sharing of confidential medical information is permitted without the consent of the patient in the event of a threat of the spread of infectious diseases by virtue of paragraph 2 of part 4 of Article 13 of the Federal Law "On the Basics of Health Protection of Citizens in the Russian Federation", photographing patients is regulated only by departmental instructions, which do not guarantee observance of rights. In particular, in Moscow the obligation to photograph patients was assigned to workers of emergency medical service teams, who were equipped with electronic devices especially for this purpose.

Facial recognition

The Russian authorities began to introduce mass video surveillance systems in the run-up to the FIFA World Cup. As part of this program, in 2015 the "Safe City" surveillance system was deployed in all regions of Russia. It is based on a plan to build a video surveillance and recording network offering the possibility of automated information exchange, video stream analysis, facial recognition and identification, as well as positioning of moving objects.

In autumn 2017, the Moscow mayor's office announced for the first time the launch of a mass facial recognition system. At the time it was stated that more than three thousand video cameras have been connected to the system, images from which are analysed in real time. Using neural networks, the system compares the faces of passers-by captured by the cameras against photos stored in databases.

All of the information captured by the cameras is transferred to the Unified Centre for Information Storage and Processing. Representatives of the law enforcement and executive authorities are able to access it from their place of work. An analysis of the Moscow legislation conducted by lawyers of Agora International demonstrates that the grounds, principles, rules and procedures for using the facial recognition technology have not been duly formulated. In particular, the following have not been defined:

- permissible cases and aims of using the technology;

- procedure for using the technology by authorised bodies (time period for using the technology, storage period of biometric data obtained, means of data processing etc.);

- mechanisms for protection of the rights and interests of subjects of personal data in the event of implementation of the technology.

This was picked up on by civil activist Alyona Popova and politician Vladimir Milov, who challenged the use of facial recognition technologies against participants in public protests in Moscow. In response, representatives of Moscow's Department of Information Technologies maintained that existing regulations are sufficient, and the technology does not violate citizens' rights.

In mid-March, the Moscow authorities reported that over 200 quarantine violators have been identified with the help of the "Safe City" surveillance system. At the same time, there has been at least one case of likely malfunctioning of the system, reported in Yuzhno-Sakhalinsk.

At present, video surveillance systems equipped with facial recognition technologies are installed in most large Russian cities. In at least 11 Russian regions and Crimea, these systems have been used to identify quarantine violators.

During the time of quarantine restrictions, the authorities in Sakhalin, Astrakhan and Belgorod regions, as well as Moscow and St Petersburg, continued to purchase additional surveillance technologies, including video surveillance and biometric data processing systems.

Meanwhile, there are concerns that access to video surveillance systems can, in all likelihood, be bought on the "black market". It seems that nothing has changed since December 2019, when journalist Andrei Kagansky succeeded in purchasing information about himself held in the database of the Moscow Unified Centre for Information Storage and Processing (ЕЦХД). As early as July 2020 an announcement appeared on the Internet offering to sell access to Moscow's video surveillance system, including the data archive.

Disclosure of diagnoses and personal data leaks

In at least 18 regions there have been reports of leaks of sensitive information, collected by the authorities as part of the struggle against the epidemic, including diagnoses and other medical information, addresses, telephone numbers etc. Most often, personal information was published in the form of lists of infected persons or those who have had contact with them, or information about individual patients' diagnoses.

In Chuvashia a list of 17 residents of the republic who have been diagnosed with COVID-19 was disseminated over messaging services – their surname, age and place of work were published.

In Bryansk Oblast a report of a married couple infected with coronavirus appeared on a social network, which included not only information about the patients, but also their relatives – including their surnames, addresses and places of work.

In Kurgan Oblast a woman who had arrived from Moscow faced harassment after her test results were published on the town's public social media page.

In Voronezh Oblast an official document of Rospotrebnadzor, addressed to the Rossoshanskaya district hospital and containing information on the diagnosis, home address and contacts of a woman who had died from coronavirus, appeared on the Internet.

In Irkutsk Oblast messages were sent with the names (including the names of minor children), address and places of work of the members of a family that had returned from holiday. According to the mother, the information was published just half an hour after they received their test results.

The online publication Mash published an interactive map of Moscow and the Moscow region showing the locations of the homes of residents who have been diagnosed with COVID-19. "Federal and regional operational headquarters to combat coronavirus" were cited as the source of information on the map. A similar map was published a little while later by the authorities of Tula Oblast, but the project was shut down following complaints from residents.

Security issues with the online fine payment system in Moscow made it possible to gain access to the passport details of fined citizens via their unique fee number, which can be matched using the programme.

The suspected data leak in Orenburg Oblast can possibly be regarded as a demonstration of the methods employed by the Ministry of Internal Affairs, which has de facto been assigned the duty to monitor compliance with self-isolation and track the movement of persons diagnosed with COVID-19, as well as those who have had contact with them. In this case, a document was disseminated over messaging services titled "List of persons placed under surveillance control as possible carriers of COVID-19". The list contained the surnames, addresses, dates of birth and telephone numbers of 277 people, and Article 19.5 of the Code of Administrative Offences (failure to follow in a timely manner a lawful instruction of a body exercising state supervision) was cited as grounds for control.

"Surveillance Control" (*Сторожевой контроль)* is a police database into which information is entered on the purchase of travel documents by persons whose movements are subject to special control. When one of these persons buys a train, air, or intercity bus ticket, the responsible police officer is notified of this. The system, created in 2005 on the basis of a secret order of the Ministry of Internal Affairs, was supposed to simplify and automate surveillance of extremists, however, as subsequently transpired during the examination by the European Court of Human Rights of the case of *Sergey Shimovolos v. Russia*, information about civil activists, human rights defenders and other persons may also find its way into the system. Decisions to enter a person into the "Surveillance Control" database are taken on the basis of "confidential information", and the procedure for taking such decisions is unknown. Thus, the automated system created to exercise

control over “suspect” citizens is probably also used for surveillance of potential spreaders of the coronavirus infection.

Furthermore, personal data leaks have been reported in Bashkortostan, Dagestan, Yakutia, Altai Krai, Volgograd, Rostov, Sverdlovsk and Novosibirsk regions, and Zabaykalsky Krai.

In all cases, the information disclosed was subject to entry in the unified database, however, the sources of the leaks (with the exception of the case involving information on fines for violating self-isolation) were, likely, persons who had access to the data – employees of the police, Rospotrebnadzor, the administrations of medical institutions, and medical workers.

The significant number of leaks confirms the need to destroy all information on citizens collected during the high alert regime (with the possible exception of anonymised data required for statistical analysis, evaluation of the effectiveness of measures taken and planning of future measures).

Since the powers to identify the contacts of patients diagnosed with COVID-19 and control over compliance with quarantine have been devolved to the regional authorities, Agora International and Roskomsvoboda, an NGO that tracks online freedoms in Russia, approached the heads of constituent territories of the Russian Federation with a proposal to guarantee the destruction of all personal data obtained about citizens within the time frame prescribed by law, with the designation of responsible officials. In respect of citizens placed in quarantine, data is to be destroyed upon expiry of the quarantine period, as regards all residents of the region – after the cancellation of the high alert regime.

In the majority of regions, the authorities considered that no special guarantees and procedures are required, citing the provisions of Article 24 of the Federal Law “On the Personal Data”, according to which data processing must cease, and the data collected destroyed, within 30 days of achievement of the aims of data processing.

Only the authorities of the Republic of Sakha (Yakutia) and Pskov Oblast declared the intention to adopt a regulation on data processing and destruction. In May, the authorities of Tatarstan announced the deletion of the database on digital passes, and soon after Minkomsvyaz announced that all data collected using the “State Services STOP Coronavirus” app have also been destroyed.

In any case, this only concerns information collected for issuing digital passes in several regions of Russia. Medical and biometric data, as well as

information on contacts, were gathered and processed separately, and the procedure for their processing and destruction is not transparent. Therefore, the risk of leaks remains significant.

Meanwhile, the Moscow government have already acknowledged that the data collected for issuing digital passes will be stored for an indefinite period of time – the destruction of such data is planned only "after the conclusion of court proceedings connected with the pass regime".

Recommendations

We recognise that the unprecedented global crisis facing humanity requires the adoption of certain extraordinary measures, and in particular may justify a degree of restriction of human rights and freedoms. The authorities of all countries must combat the pandemic, and citizens have the right to expect that governments will be able to overcome its economic consequences and stop the spread of the virus.

At the same time, we are convinced that any measures taken must be lawful, effective and proportionate, and the restriction of human rights may only be temporary and subject to public control.

We call upon the Russian authorities to refrain from excessive broadening of the interference with the right to privacy and respect for private life, and also observe the norms of international law.

We recommend observance of the following principles:

1) Any form of surveillance must be established by accessible and clearly formulated normative acts, adopted by authorised bodies within the limits of their competence.

2) The use of any tracking technologies must be voluntary and not mandatory. Forced surveillance and gathering of information on the private lives of specific persons must be sanctioned by a justified court decision, limited in time, scope and means of execution.

3) Indiscriminate mass surveillance is, in any case, unlawful and must not be used, since it does not allow for analysis of each specific case in terms of the necessity and proportionality of the measures taken.

4) Any data collected must be secured and used by authorised persons only. The state must ensure that officials responsible for disclosing personal data are held responsible, and that victims are awarded fair compensation.

5) In the event of processing of anonymised data, the corresponding state body or authorised official must be able to confirm the anonymity of such data at any time.

6) The minimum possible amount of data may be collected, and only for the purposes of protection of public health, and must not be the subject of sale (including in anonymised form), or used for any other ends, including punitive purposes.

7) All data obtained must be securely destroyed after the aims of data processing have been achieved, in each case. In particular, data obtained for the purpose of monitoring compliance with mandatory quarantine by specific persons must be destroyed after the expiry of the quarantine period.

8) Surveillance cannot be discriminatory in nature and be performed on the grounds of race, nationality, citizenship or country of origin.

9) The responsibility rests with the state to ensure the transparency of all actions and measures taken, and the creation of conditions for their independent auditing from the point of view of impact on human rights.

Damir GAINUTDINOV

legal analyst at Agora International

AGORA

—Международная правозащитная группа—

Agora International Human Rights Group is an association of dozens of lawyers from several countries, specialising in legal defence of civil freedoms in the post-Soviet space.