# Covid-1984: Surveillance in a pandemic year

Pandemic Big Brother

Роскомсвобода

pandemicbigbrother.online

# Key ideas

1 Authorities in various countries reached agreements with local mobile operators to hand-over geolocation details

2 Apps to track contacts with infected people became one of the most popular digital answers for governments looking to prevent the spread of COVID-19

3 During the pandemic, face recognition technology began to be deployed to identify those breaking lockdown rules, among other uses

4 In a series of countries, where installing a coronavirus tracking app was compulsory, refusal to install the app could be punished by a fine

5 During widespread lockdown in the spring, drones became a popular way of monitoring the observation of self-isolation

6 From April 2020 in Russia, the authorities launched 4 official apps to track contacts with infected people, issue digital permits and monitoring people who were under quarantine or undergoing home treatment

7 During the pandemic, Russian citizens received more than 1.1 million fines for breaking coronavirus-related restrictions

8 In several cases, the government coronavirus apps were obviously used to monitor people and violate the right to an inviolable private life

9 Russia’s use of a system of automatic fines for violating lockdown rules with the help of face-recognition technology and through the Social Monitoring app led to many mistakes and fines for law-abiding citizens

## Report authors

Sarkis Darbinyan
Alena Ryzhikova
Anna Karnaukhova

# With the assistance of

Human constanta

AGORA

EURASIAN DIGITAL FOUNDATION

інтернет свобода

ГРАЖДАНСКАЯ ИНИЦИАТИВА ИНТЕРНЕТ ПОЛИТИКИ

DIGITAL COMMUNICATION NETWORK

eQualitie

IFKZ Internet Freedom KAZAKHSTAN

ARTICLE 19

accessnow

# Contents

# Introduction

When it comes to coronavirus limitations linked to the use of digital technology, we have a seen a sort of race in 2020 between governments of different countries in terms of which new technologies can be used to restrict the spread of the virus. In the 9 months since we launched our interactive map, Pandemic Big Brother , we have seen sophisticated tracking methods, including drones issuing warnings about observing lockdown, 'scanning helmets' capable of measuring of people's temperature  and even the deployment of hot air balloons to find lockdown-breakers.

For the first time, the world encountered the phenomenon of a lockdown, and in order to leave their homes and visit nearby shops people were obliged to obtain digital passes and permissions.

In terms of Russia, the lockdown was first introduced in Moscow Region and Moscow at the end of March, 2020. The lockdown included a ban on leaving the house for all people, with the exception of those who needed to go to work or receive medical treatment. Other exceptions were visiting shops, chemists, and walking domestic pets. After this, a lockdown was introduced in other regions of Russia and violations were punished by new fines and other sanctions.

The pandemic justified the much wider deployment of human tracking instruments as the basis for the gathering of large amounts of data on residents of large towns — allegedly for the noble reasons of concern about life and health.

The authorities launched monitoring operations through state services, mobile telephones and CCTV systems with a face-recognition, digital passes, QR-codes, mobile apps, SMS-passes, and geotagging by mobile operators.

The data in this report about the measures taken to reduce coronavirus infections using digital technology is not exhaustive. We focus on the key instruments which, as well as being used for their official goals, were also used for monitoring people, including illegal monitoring.

# Mobile apps

## The world

All over the world, coronavirus curtailment of freedom of movement (compulsory quarantine, curfews) were accompanied by digital restrictions. As early as February-March 2020, authorities in most countries had activated their digital ministries for the creation of state apps, which could help reduce new coronavirus infections.

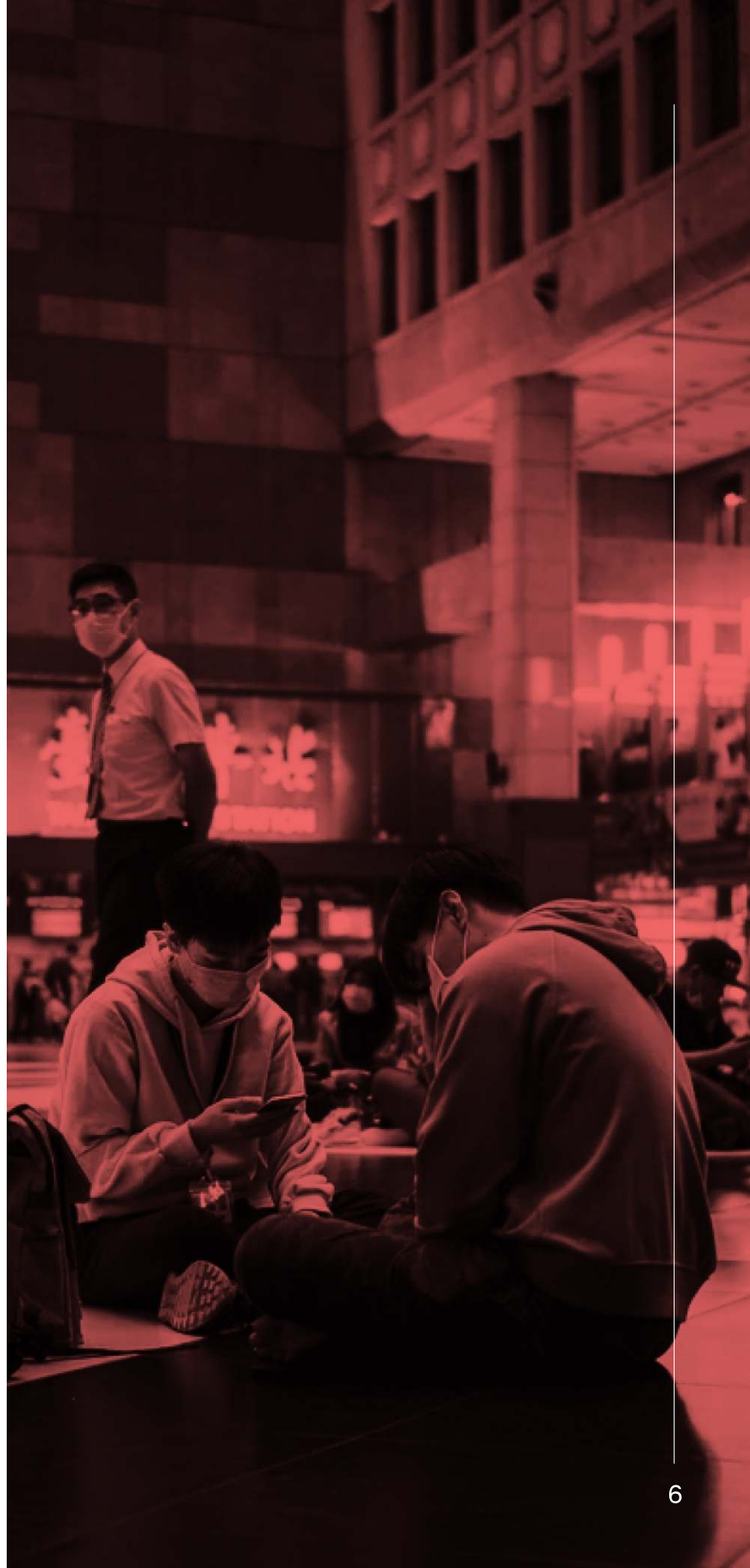
Since the launch of the Pandemic Big Brother interactive map, we have identified such apps in 116 countries. While these apps have different aims, we can divide them in the following categories:

**Information**
Provides official information about the level of infection in the region, and material about prophylactic measures.

**Self-diagnosis**
allows people to independently ‘diagnose’ their symptoms and compare them with the symptoms of COVID-19.

**Tracking contact with infected people**
using Bluetooth and GPS-tracker technology to flag contacts with other devices located nearby.

**Check observance of quarantine for those ill with COVID-19**
This requires constant access to the device’s location, and these apps can request selfies with geolocation. In some countries, aside from the compulsory installation of apps, those with COVID-19 were required to wear a special GPS-tracker.



**Issuance of digital passes and QR-codes**, which give you the right to leave your house during a lockdown.

**Used by law enforcement agencies to track** whether you have a digital pass or other forms of permission during compulsory quarantine.

As of December 2020, most of the apps for monitoring contact with those infected with coronavirus were operated on the basis of joint-development with Apple and Google APIs and worked via Bluetooth. Installation was not compulsory for all citizens. There was widespread interest in such apps, however, for the moment, there is little information about their effectiveness in reducing the spread of the infection.

Technology developed by Apple and Google uses Bluetooth signals and warns users if it has identified a contact with an app on another device whose owner received a COVID-19 diagnosis.

The data that is collected is mostly stored in a decentralised way, on the devices of the users themselves. Every day, each telephone generates a new encryption code, which is subsequently used to generate a random identification number. If the user finds out that they are infected, they can give the health authorities permission to publicly share, on a temporary basis, their access key. In this way, the users themselves remain anonymous to each other.

Access to the technology was only given to state health authorities in those countries that decide to create an app on the basis of this technology. In addition, if they created such an app, they needed to adhere to certain confidentiality criteria, and certain security and data standards required by Apple and Google.

The system passes on the data that has been collected only in those cases when the user decides to inform about a positive COVID-19 diagnosis, or if the user receives a notification that they were in contact with an infected person.

## The overall number of such state apps launched during the pandemic is more than 135

You can find out which countries launched their own apps, and details on their operation, in our table

## Not all the apps identified by us violated privacy rights, or other digital rights

But most of them, one way or another, were tracking a device's location, storing this information and passing it to other devices and third parties

Apps based on this API were used in Australia, Austria, Belgium, Brazil, Germany, Denmark, Ireland, Spain, Italy, Canada, Latvia, the Netherlands, Poland, Russia, U.S. (a different app in every state), Uruguay, Finland, Estonia, Japan and others.

It's important to flag that European apps used to track contacts, aside from a lot of care to ensure user privacy and data confidentiality, aim to be compatible with each other. The developers had in mind that borders between countries would be re-opened.

One of the first countries to launch an app to track possible contact with infected people was China. From the moment of its launch, the Alipay Health Code app was compulsory for all residents and was integrated into almost all areas of interaction: it was necessary to show your own QR 'health-code' when you visited public places, rode a taxi, booked a hotel or air ticket, and so on. All data about your location is automatically passed to the police.

The Indian government, which, to start with, developed separate apps for each state, had, by May, changed tactics and focused on one app – Aarogya Setu – making it compulsory for everyone. The absence of the app on your smartphone could be a reason to block you from using trains or public transport, and for a refusal to install the app you faced a fine of $13 or a prison term of up to 6 months. A month after the launch of the app on 2 April, it had been downloaded more than a 100 million times and entered the top-10 most downloaded apps in the world. After criticism from human rights defenders about violations of the right to privacy and the collection of confidential data, the authorities revealed that the app has an open source code.

Another of the first countries to develop a 'coronavirus app' was Singapore with its app Trace Together. Later, this app became a model for the rollout of a similar system of monitoring in other countries. This app uses Bluetooth technology and automatically deletes the data it has collected after 25 days. The data from the app is only passed to the authorities if the user has a positive COVID-19 result. By December, the app had been downloaded by over 50 percent of Singaporeans despite the fact that it was not compulsory.

For example, as far back as June, the German app Corona Warn was accessible in at least 10 European countries

Luxembourg, France, Belgium, the Netherlands, Austria, Belgium, Bulgaria, Czechia, Denmark, Poland and Romania

A series of apps launched by various countries to monitor contacts with infected people worked on a different principle: they were based on the scanning of QR-codes (such a system was launched for entertainment venues in Moscow).

At the beginning of June, South Korea switched to a system of digital passes for public places based on QR-codes. At the same time as restaurants, fitness clubs and other public places were allowed to open, their owners were obliged to put up special equipment with QR-codes, which was designed to count the visitors.

A similar system of QR-code passes was rolled out in June in Thailand . In places where large groups of people gather, and on public transport, posters apeared with QR-codes, which people were obliged to scan on a government monitoring app. Within 24 hours of this system being launched, more than 44,000 business registered.

At the end of September, an app with the option of QR-code scanning was launched in the United Kingdom. The NHS COVID-19 app allows the monitoring of contacts with infected people with the use of Bluetooth technology ; informs users about the risks of the illness based on postcode; allows registration via QR-code in public places; and allows you to check if your illness symptoms align with COVID-19 symptoms. The launch of the app was initially planned for June, but was delayed several times over confidentiality fears. Like in Thailand, posters with QR-codes were put up in public places that visitors were supposed to scan prior to their visit

Aside from South Korea, Thailand and the United Kingdom, similar QR-pass systems were also used in Hong Kong along with the government Leave Home Safe app.

Tracking contacts with infected people in such apps take place in the following way: visitors scan the QR-code and, if one of them is later found to have coronavirus, the rest receive a notification about the possibility of contacts and must quarantine.

Another type of app worth noting is that for people who are self-treating at home, or who are under compulsory quarantine.

The authorities in most countries obliged everyone returning from abroad to quarantine. In the middle of May, an app for those under quarantine was launched in Slovakia, and violators of quarantine could be fined 1,650 euros.

In April, Ukraine launched an app to control observance of self-isolation measures . In the course of 14 days, users could receive up to 10 notifications, including those that required them to take a photo.

During the pandemic in Kazakhstan, the Smart Astana app, through which people could reach the capital's contact centre for everyday questions and get a government services consultation, received a series of new functions, including the obligation to monitor people on compulsory quarantine. The authorities required everyone in compulsory quarantine to install the app and the turn-on geolocation, Wi-Fi and Bluetooth so that they could, in real time, monitor your location. If you were found to be more than 30 metres away from the point fixed as your home address, the Health Ministry received a notification and you would receive a video call to establish your location.

> Some countries did not stop at new apps, but launched a whole innovative monitoring system, including bracelets and other devices.

This was how the government of Kuwait acted, and all of its citizens returning from abroad were obliged to wear a tracking bracelet. These bracelets were integrated into a government app, which you could register using a unique government identifier. If the bracelet established that a person has exited the limits of their proscribed geolocation, the health authorities get a notification about a violation.

A similar system of an app and bracelets operates in Bahrain. However, in addition to constant monitoring of your whereabouts, the app also regularly requested selfies and confirmation that you are observing the compulsory quarantine.

In general, more severe measures for tracking people's location with the use of bracelets is something we saw in the Middle East. In neighbouring Oman, as an addition to the government app Tarassud, which informs people about the latest news on COVID-19, they launched Tarassud Plus, an app for people on compulsory quarantine and obliged to wear a special bracelet. This app automatically informs the authorities if a user breaks quarantine or tries to remove or harm the device.

> In June, human rights organisation Amnesty International released research that showed that Persian Gulf countries had launched mass monitoring of their citizens using the excuse of digital coronavirus restrictions

However, if Arab countries used systems to monitor whereabouts of people in quarantine via bracelets, then Singapore used a similar system for all the residents of the country. According to observers, the authorities required every resident to install a tracking app or wear a sort of pendent, which functioned in a similar way. From November, this was required to enter cinemas, and from the start of 2021 the absence of the app, or the pendent, will be a reason to refuse people entry to shops, the metro and other places where there are large gatherings.

> The leader of a ranking of governments who used coronavirus as an excuse to monitor their citizens through a government app was Syria

> For a refusal to install the government app in Qatar, residents could be fined up to 200,000 Qatari riyals (about $55,000), or imprisoned for up to 3 years

In April, media reports suggested that, under the guise of a coronavirus app, the Syrian government had been spreading spyware. There were also reports that government-linked hackers were using at least 71 malicious Android applications to track location, collect contact information and get access to photo and video files on personal devices.

While the governments of some countries launched suspicious apps to coronavirus that, in actual fact, are designed to track people, other governments shut down apps that interfered too much in people's private lives. One example of such a change of tactics in the fight with the pandemic is the Norwegian app Smittestopp. It was officially launched in April 2020, but, in June, the Norwegian data protection authorities ruled  that the constant monitoring of people's geolocation violated their right to a private life. The app was shut down and the data it had collected deleted.

# Russia

Since the start of the pandemic, the Russian authorities have launched four different apps, which are used to issue digital passes, monitor people under quarantine and track contacts with those infected with coronavirus.

In April, the Ministry for Digital Development launched an app that issues digital passes: ‘Gosuslugi STOP coronavirus’ . You could get authorised on it via the Gosuslugi portal and the app took an interest in the health of the user, allowed you to fill out a form and specify the reason for leaving your residence. After filling in all the required information, the app generated a QR-code and showed a ‘timer for being outside’. Other regions introduced their own digital pass systems, and to receive these passes users were sent to special websites operated by local authorities.

Moscow occupies a leading position when it comes to the number of tools for control and monitoring: from April, there was a system of digital passes that controlled people’s movements and the Social Monitoring  system monitored those ill with coronavirus. In May, the traffic police started to use the Quarantine app  in order to identify vehicles without digital passes to be outside.

The most controversial app in Russia’s lockdown was the Social Monitoring app. There were masses of complaints by Muscovites about mistakes in the way the app worked: people received automatic fines for violating quarantine, sometimes when they had never left their residences, or when their quarantine was actually over.

On 4 June, Moscow Mayor Sergei Sobyanin announced, that the city authorities were not planning to store the data collected via the systems of digital passes and the Social Monitoring app, however, they continue to be stored for an indefinite period of time. The app was downloaded by more than 400,000 Muscovites.

During the period of mass fines for violating mask-wearing rules and lockdown measures, the legal service Destra Legal launched an app to complain about unfair fines . The app contained step-by-step instructions to file a complaint against fines issued for breaking lockdown and allowed them to be sent automatically to court.

On 11 June, Aleksei Nemeryuk, first deputy chief of staff for the Moscow mayor and head of the Trade Department, stated that data on citizens collected by the digital pass system would be deleted after all legal proceedings involving the pass system have ended, which, from the point of the law, is a very undefined period of time considering the significantly different timeframes of first-instance courts and the European Court of Human Rights. At the present time, there is no information about the method of storage or when the data will be deleted, or about the formation of a special commission to track this process. Likewise, there is no clear information on the reasons for collecting this sort of data from Muscovites.

At the end of August, the head of the Health Ministry announced that the authorities had begun developing a mobile app that would track the health of Russians who had been vaccinated. Despite the fact that vaccinations in Russia began in December, there is still no information on the launch of this app.

> Even though lockdown measures were eased in Russia, the number of tools to monitor Moscow residents has continued to rise

A special requirement for entertainment venues was introduced and, from 19 October, visitors and employees of these venues were supposed to scan a QR-code and confirm their telephone number, either via a SMS, or via the so-called check-in system.

Nemeryuk, called the current system “humane” as, thanks to identification, people can evaluate the threat to their lives and get treatment quickly if they are infected.

In a decree, Moscow Mayor Sergei Sobyanin ordered all employers to provide weekly data about their staff who had been switched to home working, including their mobile numbers, their car license plates, the number of their Troika or Strelka travel cards, and the number of their social cards.

> For violating these demands, employers could be fined up to 300,000 roubles or have their businesses closed down in accordance with article 20.6.1 of the Administrative Code (ignoring rules during an emergency situation or the threat of one arising)

The Department of Information Technology stated that the Moscow authorities will not seek to restrict the movement of people whose details they received via the abovementioned measures. According to the department, this information is necessary only for an assessment of the effectiveness. The authorities also stated that four large Russian companies (Sberbank, VTB, RZhd and Mail.ru Group) handed the mayor's office the personal data of more than 35,000 of their staff members who were switched over to working from home.

Roskomsvoboda filed a complaint to the Moscow City Court with a demand to scrap the measures instituted by order of Mayor Sobyanin forcing employers to hand over data on their employees as it violated the law on personal data in the Labour Code. As this report was being compiled, a hearing had yet to take place.

The fourth app launched by the Russian authorities during the pandemic was the app 'Gosuslugi. COVID tracker' to monitor contact with those sick with coronavirus. Despite the word 'gosuslugi', it was in no way linked with the state services portal. The authorities assured users that the information collected would be anonymous. The app was built using Exposure Notification technology developed by Apple and Google, and the installation of the app – unlike Social Monitoring – was voluntary.

# CCTV and Face Recognition

## The world

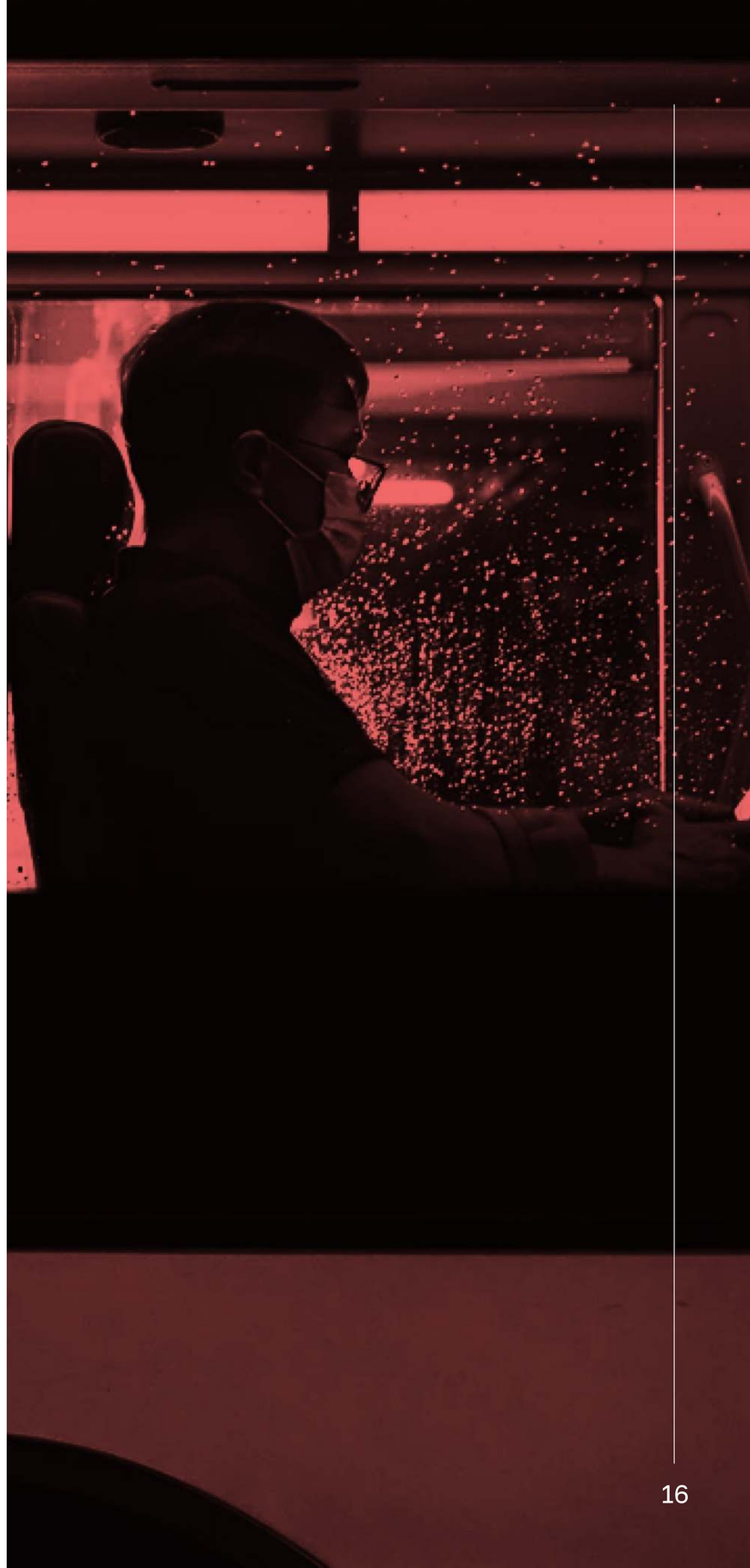
Almost from the start of the coronavirus pandemic, we noticed that governments of began to use CCTV systems with face recognition to monitor observation of self-isolation orders and catch quarantine-evaders.

In China, where face recognition software was actively used even before the pandemic, cameras tracked those breaking quarantine and self-isolation orders. The algorithms used in China, on the basis of machine learning, are able to recognise people in masks and determine their body temperatures.

When judged on the level of monitoring technology introduced during the pandemic, China is undoubtedly a world leader. The police in China were equipped with 'scanning helmets', which automatically measured the temperature of everyone nearby and could, if necessary, scan people's QR-codes. The developer company said it has already dispatched these helmets to Italy's military police and the Norwegian government for trials. This equipment was also used by police in Dubai.

In September, Japanese technology company NEC announced it had developed face recognition technology that can, with 99.9% accuracy identify people wearing masks. The company said it was ready to bring this technology to the market, however the first place it was actually employed was the company's head office in Tokyo.

> In several countries, drones were mobilised to monitor lockdown observance



These drones tracked whether people were assembling in big groups, and informed them about the necessity of self-isolation. Drones were first used in this way in China at the beginning of March. Later, this idea was seized on by the governments of Australia, Belgium, Germany, Italy, Spain, Kazakhstan, UAE and the United States.

At the end of April, the Indian authorities looked at the possibility of introducing drones with face recognition software integrated into the Aadhaar system. This is an Indian digital identification programme, based on biometrics, that boasts the details of 1.25 billion people and is likely the biggest system of biometric data collection in the world.

At the same time, the pandemic was a stimulus for the active introduction of face recognition technology in democratic countries, and international rights organisations are striving to enter a dialogue with the authorities to prove that this is an excessive measure, which violates people's right to a private life.

> If we're talking about European countries, at the present moment, **Belgium** is the only country using face recognition technology that is in breach of national law

In many countries, a system of CCTV with face recognition functioning was tested during the pandemic. In May, the French authorities launched a trial of a face recognition algorithm in the Paris metro. It was announced that the algorithm was capable of recognising faces even if passengers were wearing masks. In the United Kingdom, a pilot project for a face recognition system in shops was launched.

At the present time, the UAE authorities are introducing face recognition technology in public transport in Dubai. The city transport police issued assurances that this measure will allow them to catch criminals more effectively, however, as experience from other countries shows, face recognition can also be used to monitor people.

It’s also worth mentioning that, in the United States, a wave of Black Lives Matter protests against police violence led the biggest technology companies to stop selling face recognition technology to government agencies. This included Microsoft, IBM and Amazon. In September, another U.S. city, Portland , following the example of San Francisco, Oakland and Somerville, banned the use of face recognition technology in public places. In particular, the issue was shops and restaurants. Portland’s city authorities also banned local government agencies from acquiring or using technologies that provoke such divisive public arguments.

## Russia

Moscow in particular became a testing-ground for face recognition technology as part of a system of city-wide CCTV. In the last six months, the Moscow authorities spent almost 1.5 billion roubles  on fitting out public transport with face recognition cameras. Later, the police announced that masks do not prevent the cameras from identifying faces.

When the capital introduced a digital pass system, more than 1,000 CCTV cameras were used to enforce lockdown observance. The operator of the CCTV system became the quasi-government organisation OATI, which has the function of controlling people on compulsory quarantine by issuing automatic fines decided by an algorithm linked to face identification. A CCTV image of people is compared with a photograph that is taken during your first visit to a doctor. However, the possibility of just 74% face correlation has not stopped courts from leaving in force fines issued by OATI.

> From the start of the pandemic, over 1.1 million people were prosecuted in Russia under the administrative code for violating coronavirus restrictions

From 1 April, liability for violating lockdown was introduced to the Moscow administrative code (article 3.18.1). Punishment is a fine of up to 4,000 roubles.

More than 109,200 protocols were issued under article 3.18.1 of the Moscow administrative code. Many people were judged guilty on the basis of information from city CCTV cameras. Cases about such violations are examined without drawing up protocols of an administrative violation. To identify violations on city roads, they used vehicle license plate numbers and photos of pedestrians. Predictably, the use of such technology led to a mass of errors and, in the end, unfair and illegal fines, which are still being challenged in the courts.

According to data from Moscow City Court, more than 64,000 fines under article 3.18.1 of the Moscow administrative code were appealed. Of them:

- More than 73 decisions were overturned
- 1,250 cases were closed
- 123 fines were successfully appealed
- 13,562 were declined
- 2,213 decisions entered force
- 10,125 fine cases were closed
- 1,673 appeals were heard in court

In Moscow Region during the May holidays, police used drones  to monitor observance of lockdown, and later, with the same aim, they used a hot air balloon.

Residents of Russian regions also got a chance to experience state surveillance during lockdown. A daughter company of state corporation Rostec developed a system of video analysis  to monitor mask-wearing, which was used at a minimum in Nizhny Novgorod and Sakhalin regions, St. Petersburg and the Tatar Republic.

Like Muscovites, residents of Yuzhno-Sakhalinsk came into contact with automatic fines for violating lockdown, which were issued on the basis of data from CCTV. Here, there were also mistakes by the algorithm.

# Geotagging

## The world

Governments used location data from internet users and mobile phones to track the virus, and whether social distancing measures were working.

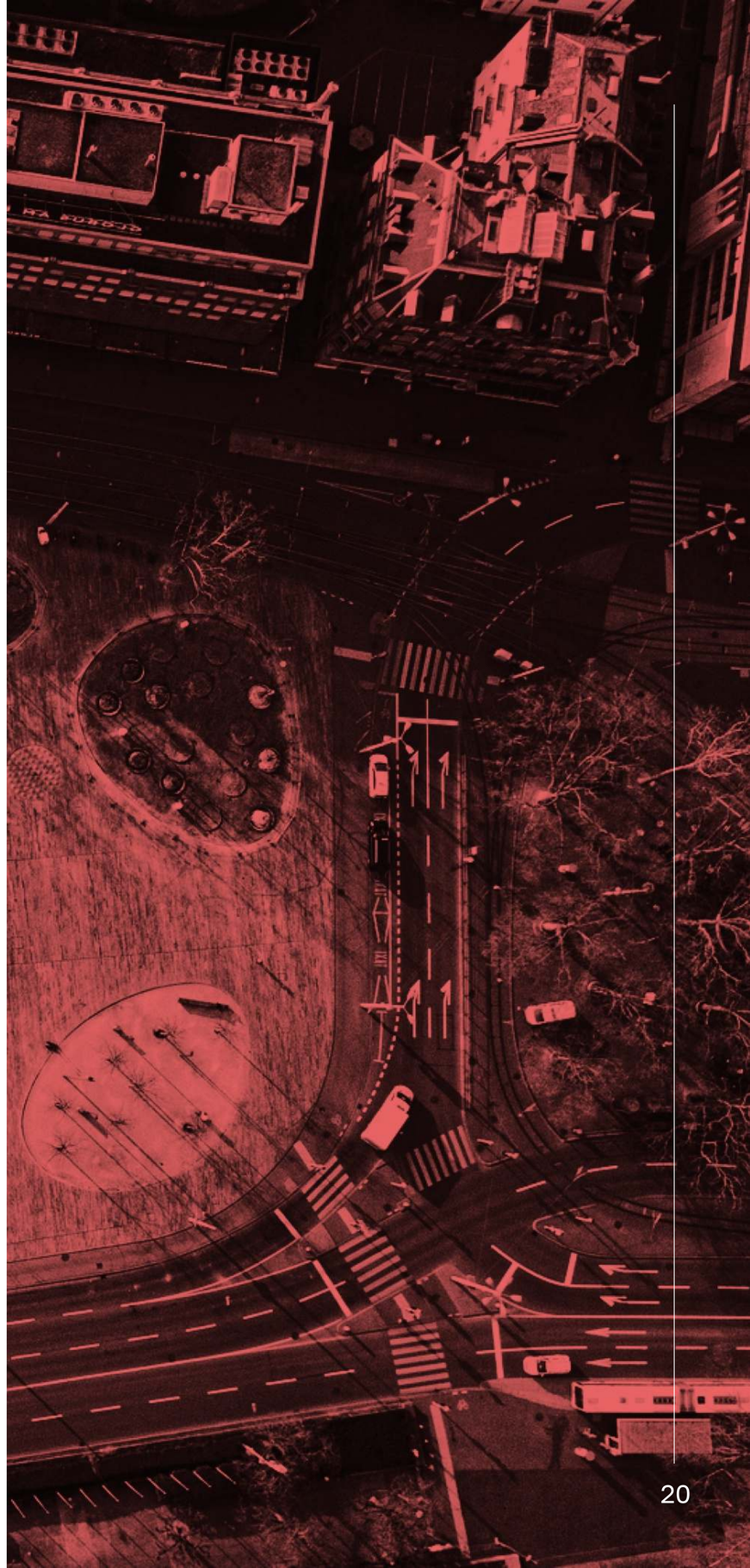
Location data can be collected in various ways, including via mobile phone operators. If surveillance takes places via Bluetooth or GPS-tracking technology on an app then the location data, in a base case scenario, is stored by the mobile phone operator.

Before the appearance of apps to track contacts with those infected with coronavirus, governments admitted they were working with local mobile operators in order to track the movements of people.

In March, one of the biggest European operators, Vodafone, confirmed it had passed data about the geolocation of its users to the government to build an aggregate, anonymous heat map of movements in Lombardy (Italy) so that the authorities could better understand population movements and stop the spread of COVID-19.

Eight European mobile operators subsequently agreed to hand the European Commission data on movement to predict the spread of COVID-19. The European Commission announced the data would be used in a depersonalised form and would be deleted once the pandemic was over.

In the middle of March, the Israeli government gave permission for its counter-terrorism and internal security service to demand mobile operators hand over data about users, including their location, and also the right to use this data to identify possible contacts with virus carriers. If contact with a virus carrier was detected, the authorities sent messages to the phone number concerning the necessity of observing quarantine.



Later, the Supreme Court decreed that, to legally deploy these warning measures, the government must pass a special privacy law that would allow such interreference in the private lives of its citizens. Even though, as early as April, the country launched an app with the same aim, the programme for gathering data location from mobile operators was only shut down in June.

At the beginning of April, the South African government announced it was going to use mobile operator data to monitor contacts with people infected with coronavirus . Doctors were obliged to supply the authorities with all the information about their sick patients, including their name, telephone number and home address.

When announcing a national emergency in March, the president of Serbia allowed the authorities to access location data of all citizens from mobile operators.

The Armenian parliament also obliged mobile operators to pass on data on users, including telephone numbers and exact location, as well as details about calls and SMS. In due course, this information was used to monitor and identify contacts with people ill with COVID-19.

With the help of mobile operators, Azerbaijan launched a system of SMS-permits. Before leaving their houses, residents were obliged to phone, or send an SMS, to a special number explaining their reason for leaving. The data collected was given to the police, who could stop people on the streets to check their permits. In December, this system of SMS-passes was reinstated after a rise in case numbers.

In April in Kazakhstan, the biggest telecommunications companies suggested the creation of a tracking system to monitor people’s movements outside their place of residence on the basis of data from mobile operators. The Akimat Department of Digitalisation in Almaty and local mobile operators reached an agreement as part of action against the spread of coronavirus. As a result of this, they created a geolocation analysis that showed the activity of mobile users and identified places where users are congregating on an hourly basis. Among the details provided by mobile operators to were the user’s call history, which suggets a violation of the constitutional right to an inviolable private life.

In Latvia, the police and the Centre for Prophylactics and Illness Control were given powers to request data about the location of people from mobile phone operators when they need to be sure of information provided by patients

> At an early stage in the spread of coronavirus, South Korea created a publicly-accessible database about cases of coronavirus, which provided detailed information about every infected person, including details on their movements based on data from mobile operators

This database was constantly updated, including with location information from card transaction histories, data from mobile phone signals and CCTV video.

The Thai authorities sought to control the places where people spent compulsory quarantine. The national Department of Cyber-Security monitored telephone signals and informed the police and local authorities if people quarantining at home left their residence or switched off their mobile phones. There is information to suggest that the police got in touch with people breaking quarantine orders within 15 minutes.

In the U.S., a company that offers mobile advertisement services cooperated with the Centre for Prophylactics and Illness Control, and also with some state governments to analyse how people's movements changed based on mobile phone location data . Google published reports on the movement of people across the world based on data collected from Google Maps. This data was passed on to the agencies responsible for predicting the spread of the illness and analysing observance of social distancing.

The gathering of location data from users was also seen in Australia , Spain , Czechia , United Kingdom , Brazil , Ecuador , Slovakia , Switzerland , China, Iran , where the government explained it as a way of defending people and reducing the risk of the development and spread of COVID-19.

# Russia

On 20 March in Russia, the prime minister ordered the Communications Ministry to develop a national system using data from mobile operators to track those who had been in contact with people with coronavirus. On 30 March, the Communications Ministry ordered regional authorities to provide a depersonalized list of mobile telephone numbers of people infected with coronavirus. Aside from those with a confirmed diagnosis, the agency also wanted the numbers of those under compulsory quarantine after returning from abroad. In the latter case, mobile operators passed on information about the country and places, the user had visited, as well as the date of their return to Russia. On 1 April, the ministry reported it had fulfiled its task.

A special algorithm creates a list of those who have been located next to an ill person, as well as those who have been in contact with them via mobile phone in the last two weeks. If the system recognises that a user has been close to an infected person for at least five minutes, then the number of that user is added to a database. If the user has been in contact with a person ill with coronavirus, then the system sends them an SMS-message. In it, the person is told they need to self-isolate. The user's data is sent to a regional operational headquarters that will track his/her location.

> The main source for state data gathering remains mobile operators

The phones of tens of millions of users send signals to a base station every five minutes. Once you place the geolocation data on a map of the city, you can get the routes of users. The margin for error, which is added by the system, is 50m to 100m.

Minister for Digital Development, Communication and Mass Media Maksut Shadayev explained how monitoring people arriving from abroad was carried out at the beginning of the pandemic. According to him, an agreement between the mobile operators and the authorities monitored the SIM cards of those returning to Russia. After this, with the help of mobile operators, the authorities determined the place to which the person had arrived and informed them of the necessity to quarantine.

# Conclusion

The instruments used by different countries to reduce coronavirus infections were not always commensurate with official aims. The rapid launch of apps for tracking contacts and monitoring people in quarantine led to apps making mistakes and information about observing quarantine, or fines, given without cause.

The year 2020 provided many new possibilities for surveillance technology and many new methods for the collection and analysis of data. The capabilities of artificial intelligence and machine learning were used by states to monitor and issue punishments for violating restrictions on movement. The data collected by many states in the Middle East and Asia corresponded neither to the principle of proportionality nor necessity. Analysis of the effectiveness of the measures to collect personal data, with a study of the correlation between infections and deaths, is the subject of separate research. However, at the present time, such figures do not exist. Among countries in the CIS region, Russia and Kazakhstan are the leaders in terms of quantity of digital technologies used to control the movement of people.

Serious risks of losing the right to a private life and examples from other countries led European society to realise the necessity of a legal consensus when it came to mass data harvesting. In October 2020, the European Court of Justice passed a significant decision that seriously restricted EU governments, including law enforcement agencies and security services, in collecting user data via mobile and internet providers, and also data storage. At the same time, the court underlined that collecting data to fight threats like coronavirus should be limited in time, and accompanied by effective oversight guarantees via courts or independent administrative bodies.

On 14 December 2020, U.K. Health Minister Matt Hancock stated that U.K. scientists had identified a new coronavirus mutation, which spreads faster than other mutations and which is 70% more infectious. From 20 December, the highest form of level-4 restrictions were implemented in London and other parts of the U.K., which means the closure of all facilities (except those selling essential goods). The list of countries that curtailed transport links with the U.K. is growing constantly.

Russia’s chief doctor, Anna Popova, extended the timeframe for sanitary-epidemiological rules to deal with coronavirus until 2022 in order no. 35 on 13 November, 2020 . Depending on the epidemiological situation, each Russian region can implement its own restrictions.

Judging by the trends at the moment of the publication, the number of surveillance methods in 2021 is set to rise. Restrictions on the rights and freedoms of people via digital technology accessed via mobile operators are unlikely to fall in the near future. Tried and tested in 2020, many of the methods described in this report will be perfected by state agencies and permanently added to the arsenal of surveillance methods.

# Covid-1984:
# Surveillance in a pandemic year

Pandemic
Big
Brother

pandemicbigbrother.online

Роскомсвобода

2020