Russia under surveillance 2017:
How the Russian state is setting up a system of total control over its citizens

Introduction

This report covers the period from May 2016 to April 2017, and continues the work of the 2016 'Russia under surveillance' report, which dealt with the variety of mechanisms used by Russian authorities for politically-motivated surveillance.[1]

Summarizing the results of the 2016 report, we concluded that the Russian state had, in recent years, organized a complex system of monitoring and surveillance of civic activists, independent journalists and the political opposition. This system, applied under the pretext of ensuring public security, combatting extremism and terrorism, is used to monitor individuals' movements within Russia and abroad, wiretaps and interception of correspondence, outdoor surveillance, covert audio and video surveillance, interception of email, collection, analysis and systematization of biometric data. In addition to these formally legal means of tracking, some manifestly illegal methods have also been used actively, such as hacking accounts of various internet services.

For the period 2007-2016, we have used open sources to document 352 separate instances of surveillance for political reasons. Most of these constitute collection of various biometric data (fingerprinting, photographing, collecting biometric data for the purposes of DNA analysis and genome registration). In 2016 and 2017 reports of new instances of data collection about activists continued to appear. However, legislative amendments and clear campaign against anonymity show us that control of non-sanctioned civil activity is just one of the objectives pursued.

The Russian authorities clearly intend to collect the maximum possible amount of information not only about all Russian Federation citizens and those who reside in the country temporarily. Now Russia's interest area includes also citizens who reside abroad on a permanent or temporary basis, owners of foreign property, bank accounts and companies, football fans and agents of law enforcement authorities.

Here, a key issue is the absolute lack of control over this surveillance. There is no public oversight, and the judicial oversight is illusory — courts automatically uphold decisions of the security services to intervene in citizens' privacy. In practice, there are no possibilities of challenging the authorities' illegal actions in court.

For instance, in the past 10 years, courts have, on average, granted 98.35% of requests concerning restrictions on citizens' constitutional rights to privacy of correspondence, telephone calls, mail, telegraph and other messages transmitted through electronic and postal communication networks.[2]

---

[1] Russia under surveillance. Report of Agora International Human Rights Group, 16 May 2016. Link: http://agora.legal/articles/Doklad-Mezhdunarodnoi-Agory-«Rossiya-pod-nablyudeniem»/2

[2] This is based on data of the Judicial Department to the Supreme Court of the Russian Federation. Link: http://www.cdep.ru

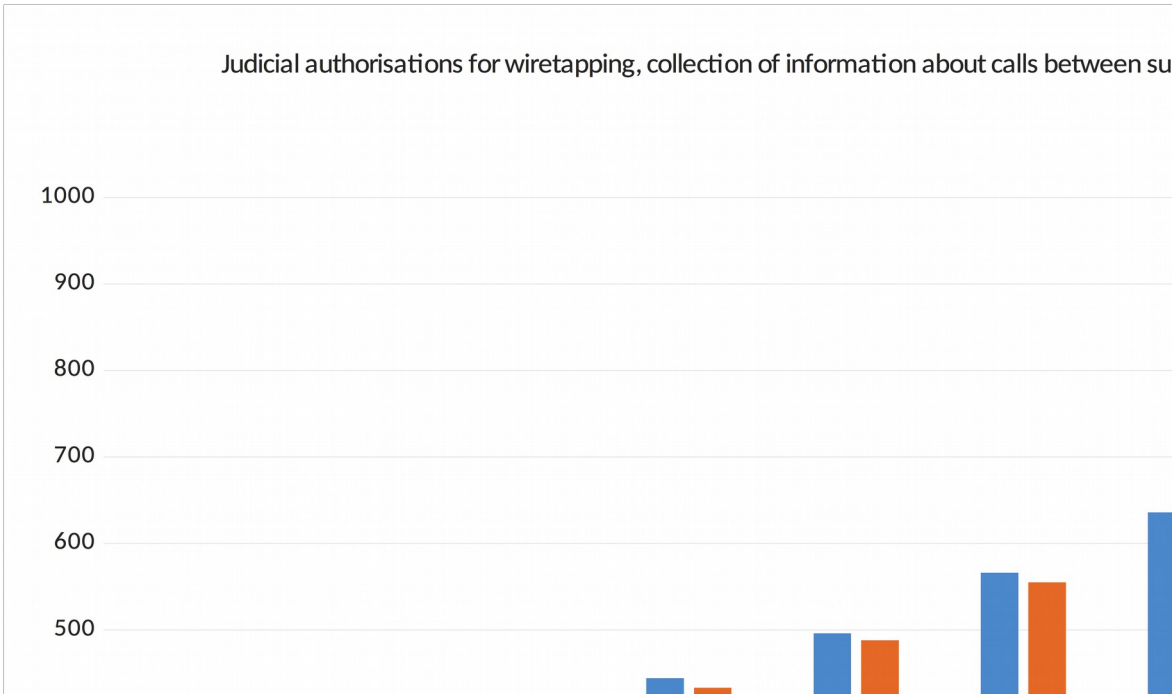
Year	Wiretapping (operative investigative measures)			Wiretapping (investigation)			Correspondence control		
	Requested	Granted (%)		Requested	Granted (%)		Requested	Granted (%)	
2007	190 485	189 591	99.53	79 698	76 346	95.79	7 342	6 983	95.11
2008	229 646	229 144	99.78	107 493	105 035	97.71	14 936	14 686	98.32
2009	246 228	245 645	99.76	132 821	130 083	97.94	17 068	16 701	97.85
2010	284 137	276 682	97.33	140 372	136 953	97.56	19 525	19 144	98.05
2011	329 415	326 105	99	144 762	140 047	96.74	21 930	21 501	98.04
2012	376 368	372 744	99.04	163 496	156 751	95.87	25 890	25 276	97.63
2013	420 242	416 045	99	189 741	178 149	93.89	25 804	25 285	97.99
2014	513 278	509 022	99.17	188 668	183 542	97.28	25 949	25 055	96.55
2015	615 683	608 192	98.78	243 792	237 439	97.39	31 825	31 021	94.33
2016	609 989	607 052	99.52	167 052	162 961	97.55	21 010	20 460	97.38
				126 306	123 092				

As a result, an ordinary legally-abiding Russian citizen is constantly exposed to the risk of arbitrary access to information about his/her private life and private data via the internet, mobile devices, CCTV in shopping centres, stadiums and other public places, in any contact with the law enforcement system, and also when receiving or spending funds, using public transport or a private motor vehicle, employment in a number of enterprises and organisations, and when exercising various rights (travelling abroad, carrying weapon, etc.).

Moreover, this data collection is justified (both formally and informally) in connection with the need to combat terrorism and extremism (in the broadest sense) as well as an individual's protest and oppositional political activity — in general, the need to combat critical attitudes towards the Russian authorities. From the state's point of view, this is a sign of inclination to criminal activity.

Thus, a citizen's right to privacy and the principle of the presumption of innocence are deprived of all meaning, and the intensity of intervention consistently

increases. For instance, the number of requests for wiretaps and interception of correspondence has tripled since 2007.



The Russian authorities are, in effect, forcing citizens to choose between taking total surveillance as a given or seeking ways to preserve their privacy. In the latter case, the state will consider this kind of behaviour illegal and will qualify it as an attempt to conceal something of a criminal nature.

In Oliver Stone's *The Putin Inteviews*, when asked whether the security services conduct surveillance of Russian citizens, president Vladimir Putin answers negatively — because Russia, in contrast to the United States, lacks the technical capacity for such operations. Insufficient resources and technical capacities undoubtedly determine the limits of state surveillance, but they do not reveal a lack of political intent or a desire to renounce efforts to collect information on Russian citizens. In fact, it is the opposite: this kind of firm denial, against the background of numerous evidence demonstrating the exact opposite, only highlights the desire to avoid unwanted public attention to this aspect of the authorities' activities.

Biometric data collection

The Russian authorities are increasingly active in their collection and use of various biometric data (fingerprints, DNA samples, photographs, etc.). According to the Federal Law on Personal Data, all such and other data indicating personally identifiable physiological and biological characteristics of a person refer to personal biometric data. This data may be collected and processed without the consent of individuals in cases provided for by Russian legislation on defence, security, combatting terrorism, transport safety, anticorruption, investigative activity, civil service, criminal enforcement legislation, laws on the requirements for entry and exit from the country, and citizenship laws.

Moreover, the Russian Federation has enacted two special statutory instruments governing the collection and processing of biometric data: Federal Law No 128-FZ from 25 July 1998 on the State Dactyloscopic Registration in the Russian Federation, and Federal Law No 242-FZ from 3 December 2008 on the State Genome Registration in the Russian Federation.

Biometrics are being more actively included in the system for identification and registration of citizens and persons visiting the country. Since 1998, a system of voluntary fingerprint registration of citizens has operated in Russia: any interested citizen may visit a branch of the Department of Interior and have his/her fingerprints taken. Furthermore, a number of categories of citizens are subject to compulsory dactyloscopic registration.

First, there is the large group of citizens who are subject to fingerprinting on the basis of their occupation: military staff, employees of the Ministry of Interior, tax and customs authorities, the Ministry of Emergency Situations, offices of enforcement agents, employees in the criminal enforcement system, the National Guard of the Russian Federation, the Federal Security Service of the Russian Federation, the Federal Security Guard Service, the foreign intelligence service, the heads of investigative authorities and investigators in the Investigation Committee of the Russian Federation, rescue workers, members of aircraft crews, applicants for a private detective license or private security certificate, naval personnel.

Second, suspects, defendants and persons convicted for criminal offences, persons under administrative arrest and who have committed administrative offences, if otherwise it is impossible to identify them.

Third, there are various categories of foreigners and stateless persons: persons subject to extradition from the country, persons who arrived in Russia as refugees, asylum seekers who have a temporary residence permit granted, persons staying illegally in the country, holders of working permits (patents).

Moreover, dactyloscopy is compulsory for persons who are unable to give details about their identity, if it is otherwise impossible to establish their identity, and for a number of other categories of persons. As of 1 January 2015, fingerprints of two fingers must also be taken of all persons aged over 12 years who have a biometric foreign travel passport issued.

Convicted persons serving imprisonment for serious or particularly serious crimes, or any type of crime against human sexual integrity or sexual freedom, are subject to DNA registration.

As we can see, this registration mechanism concerns at least 25 million people. Nevertheless, there are regular proposals to extend the application of compulsory dactyloscopic and genome registration, for example with respect to persons applying for driving licences, permits for storing and carrying weapons, patients in psychiatric and neurological clinics or drug rehabilitation centres, etc., including all citizens and persons entering the country.

In June 2016, Vladimir Putin announced plans to set up a federal information system for biometric registration that would store data about 'persons involved in terrorism and extremism'.[3] A year later, the Ministry of Interior (MoI) announced that a bill was proposed in the State Duma (the Russian parliament) on compulsory dactyloscopic registration and photographing of all foreigners, without exception, who register in Russia at their place of residence or stay.[4]

Moreover, pursuant to the law, citizens' dactyloscopic data is kept, as a rule, until they reach 80 years of age, and DNA data up to 100 years. This data may be provided to a wide range of state agencies.

Despite the detailed list of grounds for compulsory biometric registration, there are regular reports of attempts for coercive fingerprinting, photographing, saliva sampling for DNA analysis, etc., with respect to detained participants in public events, civic activists and journalists.

On 11 May 2016, in the Crimean city of Simferopol, unidentified persons in civilian clothes detained Igor Burdyga, a correspondent from the RBC-Ukraine periodical. The journalist was taken to a police department where his fingerprints, shoe prints and saliva samples were taken. Thereafter, agents from the Federal Security Service interviewed him for seven hours, threatening to initiate criminal proceedings against him and to arrest him in a pretrial detention facility. Burdyga was questioned about the purposes of his foreign travels and acquaintance with activists and journalists from Crimea.[5]

On 26 July 2016, in Moscow, civic activist Vasiliy Nedopekin was detained. The previous day, Nedopekin had participated in an event in support of political prisoner Ildar Dadin. In the Dmitrovskiy branch of the Department of Interior, police officers attempted to take his fingerprints and photographs of him.[6]

On 23 March 2017, in Moscow, police officers detained 11 supporters of Aleksei Navalny, who were distributing stickers in support of his campaign to be allowed to take part in the Russian presidential elections. They all were taken to the Arbat Department of Interior for a prophylactic talk, during which their passport data and fingerprints were recorded and taken respectively.[7]

Raids against Crimean Tatar activists in Crimea still continue. On 6 April 2017, the Russian OMON Special Task Force cordoned off the Central Market in Simferopol and thereafter security officials detained roughly50 people of 'non-Slavic appearance'. Edem Semedlyaev, a lawyer, reported that all detainees were subject to dactyloscoping, photographing and DNA sampling. Those who refused to have their samples taken were kept in the police department.[8]

---

[3] Putin announced the set-up of a database of terrorists and extremists. Link: http://bit.ly/2uIXhQA

[4] Recognised by fingers. Link http://bit.ly/2uHVi0r

[5] How I was a spy: a reporter from RBC-Ukraine spent a day in the FSS in Crimea. Link http://bit.ly/2uo5U5X

[6] An activist detained at his home was forced to undergo dactyloscoping. Link: http://bit.ly/2uWHwIq

[7] Eleven supporters of Navalny were detained in Moscow while distributing stickers. Link: http://bit.ly/2uYjL25

[8] Russian media learned about mass arrest at a Simferopol market. Link: http://bit.ly/2w8sjAP

Video surveillance

Since 2015 a video surveillance system called 'Safe City' has been deployed in all Russian regions. In Moscow alone, the amount of RUB 184.5 billion (£2.4bn) is intended to be spent for the development of this program from 2012 to 2019.[9]

The concept of the programme was approved by Government Decree No 2446-r (3 December 2014) and is based on the plan to build a branched system for video surveillance and video fixation allowing automatic exchange of information, an analysis of video streams, recognition and identification of faces and location of moving objects.

For instance, according to the report on the implementation of the program in Moscow in 2016, 86.3% of the residential city area is covered by video surveillance systems, and at the beginning of the reporting period 128,598 CCTV cameras were installed in Moscow, of which more than 98,000 cameras were installed at entrances to apartment buildings. A video images archive is kept for five days and direct access to such images is allowed not only to Interior Ministry officials, but also other executive authorities.[10]

In Nizhny Novgorod, it is planned to include pre-existing video surveillance systems at transport, sport and commercial facilities, hotels, etc. in the Safe City programme. Part of them will be equipped with systems for recognition of faces and reading motor vehicle plates.[11]

Under the pretext of preparing for international sporting events (2017 FIFA Confederations Cup and 2018 FIFA World Cup), the Russian authorities are strengthening safety measures, extending and improving surveillance systems. Sports facilities are being equipped with video face-recognition surveillance systems, even in cities which are not hosting events. These systems are already operating or are being deployed in Sochi (Fisht), Kazan (Kazan-Arena, Tatneft-Arena), Moscow (Luzhniki, Otkritie), Voronezh (Chaika and Lokomotiv), Saint Petersburg (Petrovskiy and Zenit Arena), Yekaterinburg (SKB-Bank Arena and Tsentralni), Novosibirsk (Zarya), Rostov-on-Don (Rostov Arena), Kaliningrad (Baltika Arena), Volgograd (Pobeda), Saransk (Mordovia Arena), Togliatti (Lada Arena), Samara (Yubileyni).

These systems are being installed not only at sport facilities. For instance, at Moscow railway stations, the authorities are extending the operation of facial recognition and vehicle license recognition systems.[12] In Moscow, plans are also made to provide access to images from Safe City CCTV to volunteers involved in the 2018 FIFA World Cup.[13]

[9] Link: http://drbez.mos.ru/bezopasnyy_gorod/

[10] An integrated video surveillance platform has been set up for the 2018 FIFA World Cup in Moscow. Link: http://bit.ly/2uvMKqb

[11] Video surveillance in Nizhny Novgorod will be included in the *Safe City* system before 2018 FIFA World Cup. Link: http://tass.ru/sport/4012160

[12] Safety systems at Moscow railway stations are being modernised. Link: http://bit.ly/2u7zGXT

[13] Volunteers at 2018 FIFA World Cup may get access to the Moscow video surveillance system for the purposes of their involvement in the tournament. Link: http://bit.ly/2hyS37a

According to Government Decree No 272 (25 March 2015), regional state institutions and municipalities are required to draw up lists of places where people gather en masse, and these include any places capable of holding more than 50 people. All such places must be equipped with video surveillance systems that can ensure constant control of the site, as well as archiving and storing records for 30 days.

Even stricter safety measures are provided for sports facilities. In accordance with the "Requirements for Counter-Terrorism Protection of Sports Facilities", sporting facilities where more than 100 persons may be injured in case of a terrorist attack must be equipped with facial recognition systems.

Special systems that can identify individuals are used at public events permitted by the authorities. During preparations for a rally on Andrei Sakharov Avenue in Moscow on 12 June 2017, Mosocw city officials stated that they intended to install facial recognition cameras (plus an indexing system) at the entrance of the area designated for the rally.[14] Thus, all citizens crossing the checkpoint on Andrei Sakharov Avenue could be identified. It should be noted that for many years, law enforcement agents (mainly from the Interior Ministry's Centre for Combatting Extremism) keep video records of all protest public events so that participants and organisers could be identified.

As of 2012, it is forbidden for participants of public events to conceal their faces behind masks or otherwise, and the review of this ban probably resulted in the only liberal measure concerning surveillance. The aforementioned provision of the Federal Law on Assemblies, Meetings, Demonstrations, Marches and Picketing was amended by the Constitutional Court of the Russian Federation after a complaint lodged by participants in the Day of Silence in Samara, who were fined in 2014 for covering their mouths with tape as a sign of protest against the silencing of discrimination and violence faced by Russian LGBT people. The Constitutional Court confirmed that the general ban to conceal one's face is required by 'the need to identify participants in public events so that to maintain the safety and public order, to protect citizens' rights and freedoms, especially during mass public events'; however, concealing one's face (or a part thereof) by participants in such events is not necessarily related to their intention to hinder personal identification, but may be due to weather conditions or medical reasons or may constitute a form of expressing an opinion that should be taken into account by both the organisers of the event and the police.[15]

Movement registration and tracking. Control of foreigners

[14] Face-recognition cameras will be installed in Moscow for a rally to be held on 12 June. Link: http://bit.ly/2uymFXF

[15] See Ruling No 1428-O of 7 July 2016 of the Constitutional Court of the Russian Federation. Link: http://bit.ly/2vbNV1v

When buying a ticket for public transport, accommodation in a hotel, using a public Wi-Fi access point in Russia, every Russian resident informs the authorities of his/her location.

In accordance with the laws on transport safety, the Russian Ministry of Transport maintains a set of automated databases of personal data of passengers travelling by practically any kind of transport: air, long-distance railway, maritime, river or road transport (international or interregional transportation). These databases include information obtained during ticket operations (booking, sale, return, check-in, boarding) and production of passenger lists. During any of the above mentioned actions, the authorities – in a constant mode of direct access – are informed of at least the passenger's full name, date of birth, type and number of identity document, gender, citizenship, points of departure and arrival, itinerary of travel.

When travelling by rail, the number of seat, carriage and train, details about the point of sale, the date and time of arrival are also specified. When travelling by air, details are given about the booking number, the date and time of arrival at the point of destination. Bus journeys include the route number, seat number, the date and time of ticket sale, the name of cashier (number of terminal), the make and registration number of the motor vehicle.

Airlines are required to submit details about flight registration at least 15 minutes prior to the flight — and in case of booking (sale) of tickets at least 24 hours — to the system.

A common practice is scanning the passports of guests in hotels, sanatoria, camping sites and other similar places. The reason for this practice is that the 'Rules for Registration and Deregistration of Citizens of the Russian Federation at Their Place of Stay or Residence in the Russian Federation' oblige hotel staff to inform the Interior Ministry within 24 hours of citizens' registration at their place of stay based on their identity documents.

The data collected is, in general, sufficient to know at any time the location of a citizen who uses any of the above mentioned means of transport or accommodates in a hotel. This data is also used to monitor movements or put pressure on civic activists or human rights defenders.

On 6 October 2016, Elena Denisenko, a lawyer, travelled by bus from Makhachkala to Krasnodar. At the administrative border between Chechnya and Dagestan, police officers made her get off the bus and questioned her for 30 minutes about the purpose of her journey and the cases she was working on. According to the police officers, the instructions for detaining and interviewing Denisenko were given by Dagestan's Interior Ministry.[16] In December 2016 this situation was repeated,[17] and according to Denisenko she was detained at the borders between Dagestan and Chechnya and the Stavropol Region three times in total: 'Further to my written inquiry to the Interior Ministry and the Federal Security Service Directorate, the Interior Ministry of

[16] Denisenko explains her detention by the Dagestan authorities with her professional practice as a lawyer. Link: **http://www.kavkaz-uzel.eu/articles/290918/**

[17] The lawyer was detained because of his professional registration. Link: http://bit.ly/2v01wtk

Dagestan sent no answer at all and the Federal Security Service Directorate replied that they had no data available about my registration. The same day I set off to Krasnodar and they made me get off the bus again, but this time for another contrived reason, i.e. on the pretext that I had two Russian passports. And none of my explanations at the border point or anything else helped until an agent from the Federal Security Service Directorate received an answer by the "initiator of my detention" (as they called it) about how they should proceed with me.'

Alexander Popkov, a lawyer from the Agora International Human Rights Group, also reported about the increased vigilance of police officers: 'From 31 January to 2 February 2017 I took part in a circuit session of the Krasnodar Regional Court on criminal proceedings against an officer from the section responsible for cases of minors at the Department of the Russian Ministry of Interior in the town of Goryachy Klyuch. Among other witnesses, during the court proceedings a number of police officers were interviewed, including from the criminal investigation office. On 3 February 2017, at about 7 a.m., I was returning from Goryachy Klyuch to Sochi. At the railway station, I was approached by police officers, including from the criminal investigation office, who mentioned that I "am of operational interest". Moreover, the operational agents stated that I was included in a "database of the Russian Interior Ministry", they knew about my itinerary and the means of transport I used, details of my identity documents and residence; they were interested in the purpose of my arrival in Goryachy Klyuch. Further to my application, the court sent an inquiry to the said police department, however they replied that I was not registered in any databases.'

In November 2016, Alexander Peredruk, a human rights defender, arrived in Saint Petersburg by plane from Moscow. He was met by police officers on the plane itself, who stated that he was included in a 'database' as an 'extremist' and a notice was sent to them by the Centre for Combatting Extremism of the need to find out the purpose of Peredruk's visit to Saint Petersburg, his phone number and the address where he intended to stay.[18]

In all of these cases, the Russian security services had precise information about when and where the person of operational interest would appear.

The Russian security services pay special attention to monitoring the movements of foreign citizens who, in certain cases, include members of Russian non-profit organisations. Thus, in October 2016, Pavel Chikov, one of the authors of this report, found special instructions for staff in a hotel in Segezha, Karelia. According to this document, hotel personnel are required to 'immediately submit to the responsible agent information they may come across about the following categories of persons:

1) Agents from foreign diplomatic missions;

[18] *Alexander Peredruk*. About current adventures at Pulkovo. Link: http://besttoday.ru/posts/14755.html

2) Representatives of Russian or foreign public bodies, non-profit or non-governmental organisations;
3) Members of official foreign delegations;
4) Representatives of foreign media;
5) Foreign experts in different fields (scholars, faculty from higher education organisations, technicians, etc.);
6) Military staff and foreign law enforcement agents;
7) Descendants from countries in the Asia-Pacific Region, the Middle East and Africa, the North Caucasian Region of the Russian Federation.'

It is worth mentioning that one of the directions of the abovementioned Safe City program is to 'warn and prevent violations of migration laws', the task of which task is 'to reduce irregular migration, to accumulate full, truthful, operational and up-to-date information about movements of foreign citizens'. This supposes total monitoring of all foreigners staying in Russia.

Another new project concerning surveillance, to a certain extent, is the Platon system for collecting fees from heavy goods vehicles. All vehicles of total permissible mass more than 12 tons must be registered in the system and install an on-board device with a GSM communication module and GPS and ERA-GLONASS navigation modules, or must have a route map. A system operator receives data about the registration number of the vehicle, the planned and actual route and, in case of using an on-board device, real-time details about the location of each vehicle. By July 2016, 530,000 on-board devices had already been installed.[19]

Administrative supervision and prophylactic registration

On 17 May 2017 amendments were adopted to the Criminal Code of the Russian Federation, the Federal Law on Administrative Supervision over Persons Released from Places of Imprisonment, and other instruments containing provisions for the administrative supervision over persons serving sentences for crimes of an extremist nature, including articles 205.2 and 282-282.3 of the Criminal Code of the Russian Federation. Based on these amendments, for example, Rafis Kashapov, a Tatar activist recognised as a political prisoner from the town of Naberezhnye Chelny who was convicted in 2015 to three years imprisonment for making publications criticizing the Russian aggression against Ukraine and violations of the rights of Crimean Tatars, was placed under administrative supervision for eight years by Ukhta City Court in the Komi Republic.[20]

This means that after his release from prison, Kashapov will have to promptly go to his place of residence and register with the local branch of the Ministry of

[19] http://platon.ru/ru/front-page/15-07-2016/5570/

[20] The Tatar human rights defender convicted for posts in social media was placed under administrative supervision for eight years. Link: http://bit.ly/2tX9XWK

Internal Affairs within three days. Thereafter he will be required to report to the competent authorities all his journeys, changes of address, employment, change of employment, dismissals, to give explanations to police officers upon request, and to appear before the representatives of the Ministry of Internal Affairs upon convocation. Police officers, in their turn, may conduct individual 'preventative conversations' with him, require details from his employer about his conduct, have unimpeded access to his home, allow or ban short-term exits from the territory defined for his residence, for instance in case of death or disease of a close relative or in connection with employment.

Any breaches of the conditions of the administrative supervision would result in criminal liability under article 314.1 of the Criminal Code of the Russian Federation which provides for imprisonment for up to one year.

This type of administrative supervision is an explicit form of surveillance and control of the conduct of 'unreliable' persons, provided that they have been previously brought to justice for a criminal offence.

However, there is also an implicit form of such control in the form of being placed on the prophylactic register. Formally, prophylactic registration is a part of the routine operation of district police officers aimed to prevent offences. In practice, it turned into a manner of control over the life and activity of 'suspicious persons' that include not only persons released from penitentiary institutions and having a non-cancelled or non-expunged conviction for serious or particularly serious crimes (which, as of late, also include crimes of an extremist nature), persons registered in drug rehab medical establishments, but also citizens who have committed administrative offences against the governmental order or the public security during mass events, and also members of 'informal youth unions'.

For example, after the administrative arrest of Andrey Chupishev, a resident of Krasnodar who was detained at a protest on 26 March 2017, he was placed on the prophylactic register as a participant in a non-sanctioned public rally.[21]

However, the best known in this regard is Dagestan. On 21 April 2017, the Memorial Human Rights Centre reported that law enforcement agents in Dagestan require citizens on the prophylactic register to provide copies of their identity documents and details about their family members.[22]

Earlier, Maxim Shevchenko, a member of the Presidential Human Rights Council of the Russian Federation, stated that prophylactic registration in Dagestan included 20,000 persons who are subject to constant inspection and checks, including when crossing the administrative border of the republic.[23] The reasons for prophylactic registration may be various: from physical appearance to participation in protests.

---

[21] 'We will spend the night at your front door.' The Krasnodar resident had prophylactic registration made in the police for his participation in a rally on 26 March. Link: http://bit.ly/2uWIEeP

[22] Human rights defenders state that collection of data about persons having prophylactic registration in Dagestan is illegal. Link: **http://bit.ly/2tJlicR**

[23] 'Maxim Shevchenko told the President about lawlessness in Dagestan'. Link: http://bit.ly/2ux1Wqi

By the way, in July 2016, Sergey Petryakov, head of the Zona Prava (Zone of Rights) human rights organisation, was also subjected to personal inspection with a documents check and identifying the purpose of travelling through the border between Dagestan and Kalmykia. Then the police officers stopped all motor vehicles entering or exiting Dagestan. Mention should be made that, for instance, at the same time it became known that the police of the republic started issuing warnings to the registered residents of the inadmissibility of any extremist activity and required them to notify the authorities of any changes of their addresses or exits from Dagestan.[24]

A year later, Memorial reported a letter received from an investigator from the district directorate of the Department of Russian Ministry of Interior in the Buynaksky District of Dagestan, which informed that prophylactic registration with respect to a certain category of supporters of non-traditional Islamic branches had been ended.[25] However, we are of the opinion that this only refers to a change in the system of organisation of such registration and there is no credible evidence of actual termination of this practice.

Registers of citizens and organisations, lists of disloyal citizens

In addition to the prophylactic registration, the Russian authorities keep a number of different registers and databases of 'non-reliable' persons and organisations. Being registered on such a list guarantees increased attention from law enforcement authorities, constant checks, detentions and inspections.

The number of 'black lists' kept by Russian law enforcement and control authorities is so large that they should be described in detail and analysed individually. Some of the lists are mentioned below.

The Federal Financial Monitoring Service (Rosfinmonitoring) publishes a 'List of organisations and individuals which/who are reportedly involved in extremist activity or terrorism'. It includes names, dates and places of birth of individuals, details about organisations. Inclusion in the list does not require a court decision banning the organisation or a conviction finding a person guilty of extremism or terrorism.[26] A prosecutor's ruling or a decision of the Ministry of Justice ceasing the activity of an organisation is sufficient to be included in the list. For individuals it is sufficient to have charges brought or a report of existing suspicions of crimes under 22 provisions of the Criminal Code, including the most 'popular' anti-extremist articles: 205.2 (approving terrorism), 280 (public calls for extremist activity), 280.1 (public calls to violate the territorial integrity of the Russian Federation), 282 (inciting enmity). Currently, 7,558 Russian citizens, 411 foreigners and 182 organisations are included in the list.

[24] Dagestan registers movements of citizens. Link: https://www.kommersant.ru/doc/3047649

[25] Human rights defenders: The repeal of prophylactic registration in Dagestan is victory of the civil society. Link: http://www.kavkaz-uzel.eu/articles/305124/

[26] Link: http://www.fedsfm.ru/documents/terr-list

Besides the above mentioned information, the Federal Financial Monitoring Service also receives passport details, data about citizenship, the place of residence or stay. Inclusion in the list means total control of financial transactions or disposal of property. The Federal Law on Countering Legalisation of Illegal Earnings (Money Laundering) and Financing of Terrorism allows persons included in the list to spend up to RUB 10, 000 (£130) per family member per month, but in practice even receiving such insignificant amounts gives rise to issues.[27]

It should be noted that details of persons excluded from the list are not subject to removal, and information regarding the suspicion of a person's involvement in extremist or terrorist activity continue to be subject to open access.

After the adoption of the Law on Foreign Agents, the Ministry of Justice started publishing the relevant list on its website.[28] Despite the authorities' assurances that the 'foreign agent' label is just a technical term and includes no negative content,[29] organisations included in the list constantly face new restrictions because of their status. In particular, they are banned from monitoring elections or supporting (criticizing) candidates, or from otherwise becoming involved in election campaigns. 'Foreign agents' are required to submit additional reports on their property, fund spending, management bodies.

Besides the list of foreign agents, the Ministry of Justice keeps lists of 'unwanted'[30] and 'extremist'[31] organisations, which contain 11 and 61 names respectively.

Recognising an organisation as 'unwanted' or 'extremist' automatically requires law enforcement authorities to identify tembers of the organisation in question. Where the issue concerns large organisations, tens of thousands, and sometimes hundreds of thousands persons find themselves under the threat of purposeful collection of information so that to be included in the 'black lists'. Thus, after a ban and coercive liquidation of the Jehovah's Witnesses organisation in 2017, some 150,000 followers of this organisation in Russia were placed on investigation lists, with possible criminal proceedings.

Likewise, the Federal Security Service and the Interior Ministry's Center for Combatting Extremism collect information about supporters of Hizb ut-Tahrir, Tablighi Jamaat, followers of Said Nursî, members of the National Bolshevik Party, the Army of People's Will, and other organisations recognised by the Supreme Court of the Russian Federation as extremist entities.

---

[27] Aleksey Glukhov. Repost, extremist, prisoner and poor. Link: https://openrussia.org/media/704646/

[28] http://unro.minjust.ru/nkoforeignagent.aspx

[29] In particular, the Constitutional Court of the Russian Federation ruled: 'any attempts to find negative contexts in the expression 'foreign agents' – moreover, based on stereotypes formed in the Soviet period, which actually have lost their meaning in the contemporary realities – are deprived of any constitutional legal grounds.' See Ruling No. 10-P/2014 of 8 April 2014 of the Constitutional Court of the Russian Federation. Link: http://doc.ksrf.ru/decision/KSRFDecision158063.pdf

[30] Link: http://minjust.ru/ru/activity/nko/unwanted

[31] Link: http://minjust.ru/ru/nko/perechen_zapret

The authorities pay increased attention wto groups which previously at the margins of social life, such as football fans. During the preparations for the 2018 FIFA World Cup, law enforcement authorities have increased their work with football fan groups. 'Police officers themselves also told about their activity regarding football fans ahead of the 2018 World Cup. In an interview, Colonel Yuriy Kolos, Head of the Interpol National Bureau with the Interior Ministry's Main Department in Moscow, reported that special measures are being taken with respect to fans. Reports on work with teenagers 'who also include sport fans' are published on websites of the Department of Interior. During joint meetings, the police require the management teams of stadiums to install video surveillance systems as needed for the law enforcement agents. Within the preparation work for the World Cup, departments consisting of 'several officers' have been set up in each regional directorate and in the territorial Department of the Russian Ministry of Interior to work with football fans,' *Mediazona* reported at the beginning of 2016.[32]

After the 2016 amendments to the Federal Law on Physical Culture and Sports in the Russian Federation, the MoI started publishing lists of persons who have a ban to visit sport events.[33] As of 24 July 2017, the list includes 319 names. For the identification of these persons, face-recognition video surveillance systems have been installed at large sport facilities.[34]

On 12 July 2017, the Russian parliament ratified the Council of Europe Convention on an Integrated Safety, Security and Service Approach at Football Matches and Other Sports Events.[35] The agreement provides, *inter alia*, that the governments will collect and exchange information about illegal activity, possibly including personal data of suspicious citizens. Thus, details about fan group members and data of citizens detained at sport facilities will most probably be accessible for security services in most, at the least, European countries.

One more group subject to special control, mostly by branches of the Ministry of Internal Affairs, are high school students. For instance, the Methodological Recommendations issued by the Ministry of Education concerning the prevention of distribution of criminal subcultures contain the following proposal: In case members of such subcultures are identified among students, agents from departments responsible for cases of minors must be immediately notified. Particular focus is put on the fact that supporters of subcultures are inclined to conspiracy, using 'uncontrollable' Internet services and encrypted means of communication. Teachers are advised to identify such persons and notify the Ministry of Internal Affairs accordingly. In other words, the role of investigator is delegated to teaching staff, and involves subsequent submission of details about minors' private and

[32] Maxim Solopov. Around football: Proceedings against CSKA and Spartak hooligans and competition between MoI departments regarding their right to counter fans. Link: http://bit.ly/2viXP1v

[33] Link: http://bit.ly/2u1VIel

[34] Natalia Goloburdova, Angelina Golovataya. The 'Big Brother' coming from KGB background arrived in Kazan: still on the Tatneft Arena only. Link: http://bit.ly/2vlofOn

[35] Link: http://bit.ly/2ubWDJn

family life to the police. This in its turn means inclusion of students in certain registers and different police databases.

Attack on anonymity. Cracking accounts

In 2016, the Russian authorities started actively combatting anonymity on Internet. The packet of counter-terrorism legislation ('Yarovaya packet') – requiring operators of mobile communications and Internet services to store records of calls, text messages and images, sounds and videos transmitted through the communications networks for six months, as well as metadata for one year, and to submit to the Federal Security Service 'information necessary to decode received, transmitted, delivered and (or) processed electronic messages' – could ensure full and unimpeded access of the security services to all users' communications if there were not the restrictions of some services and end-to-end encryption technologies.

The Yarovaya packet (this refers mainly to Federal Law No 374-FZ of 6 July 2016 on the Introduction of Amendments to the Federal Law on the Counteraction of Terrorism and to Certain Legislative Acts of the Russian Federation with Regard to Establishing Additional Measures Designed to Counteract Terrorism and Promote Public Safety), is, to a certain extent, a continuation of the course adopted by the Russian authorities in 2011-2012 towards nationalisation and deanonymization of the Russian internet, which may secure total control over information flows within the country.

The Ministry of Communications and Mass Media (MinComSvyaz) already published plans[36] according to which, by 2020, 99% of Internet traffic would be within the country and the Law on Localisation of User Data would apply (Federal Law No 242-FZ of 21 July 2014 on Amendments to Certain Legislative Acts of the Russian Federation to Clarify the Procedure of Personal Data Processing in Information and Telecommunication Networks), which would require Internet services to store personal data of Russian citizens physically on Russian territory.

Storing vaguely defined personal data separately from other users' information is economically unjustified. It also carries the risk of blocking and administrative liability based on an arbitrary decision of the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor). It is likely that the authorities believed that companies would ultimately prefer to transfer all data of Russian citizens on to Russian territory, which, coupled with the requirement to notify the authorities of the location where this data is stored, would significantly facilitate the access of the security services to servers. Currently, however, the larger part of the most 'interesting' services from the point of view of the security services (Google, Facebook, Apple, Twitter, Telegram, WhatsApp) have not consented to this physical data transfer.

The next step is the Law on Messengers and the Law on Anonymizers signed by Vladimir Putin on 30 July 2017. The first provides for compulsory identification of

[36] Pavel Kantishev, Anastasia Golitsina. Runet will be completely separated by 2020. Link: http://bit.ly/1Xowq5E

users based on their mobile phone number and the possibility of blocking accounts upon request by authorities.[37] The second law formally prohibits services allowing circumvention of blocking, but is actually an attempt to put anonymizers and VPN services under the control of the Federal Security Service.[38]

In August 2017, the Ministry of Communications and Mass Media (MinComSvyaz) published a draft of the requirements for the equipment and software of Internet services, which was submitted to the register of information distribution organisers.[39] What is of greatest interest is the list of users' data that must be accessible to the Federal Security Service, which controls SORM ('System for Operative Investigative Activities'): user's identifier, date and time of registration, date, time and number of agreement (if any), nickname, date of birth, address, given name, father's name and surname, passport details, identifiers of other personal documents, user's languages, details about relatives, information about accounts in other Internet services, date and time of latest update of registration details, date and time of termination of user's registration, information about receiving, sending and processing text messages, images, sounds, other messages, addressees' details, monetary transactions, including details of payees, payment system, amounts, currency, paid goods (services), client software used, geolocation data, etc.

It should be noted that pursuant to law, services are required to store and submit to the special services not only sent and received messages, but also draft messages.

The vague wordings of laws, which is freely interpreted by the relevant governing authorities, have resulted in a situation where Internet services are faced with the choice between protection of their users and cooperation with the Russian authorities, which constantly increase the pressure on them and make more and more requests. Anonymity has pushed out the blocking of 'unlawful' content to become a key point in the relationship between Internet services, users and the state.

As public opinion surveys indicate, currently most Russian citizens do not take due care in maintaining their privacy. According to Levada-Center, 49% of interviewees are not concerned that other people may get access to their data transmitted via Internet or telephone networks, and 41% have a positive view of the idea to ban the use of nicknames on Internet.[40]

Nevertheless, for civic activists, independent journalists and political opposition figures, the refusal of internet companies to cooperate with the Russian authorities, as well as their resistance to hacking, has actually become the only guarantee of safety and a key factor determining the choice of a service.

Being accused of cooperating with the Russian authorities is damaging for a business' reputation, and forces companies to justify themselves, such as the

[37] Link: http://bit.ly/2vlafat

[38] Link: http://bit.ly/2f1bxAg

[39] Link: http://regulation.gov.ru/projects#npa=18013

[40] Personal data safety survey. Link: http://bit.ly/2hgLMfY

developer of the protected Theema messenger, which had to persuade its users that 'we are not allowed and we ourselves do not wish to provide any data of our users to foreign authorities'.[41]

The public discussion that arose against the background of the dialogue between Alexander Zharov, the head of Roskomnadzor, and Pavel Durov, the creator of Telegram, about the inclusion of the service in the Register of Information Exchange Organisers is telling.[42] Observers were equally of the opinion that the real aim of the authorities, despite Zharov's statements, is accessing users' correspondence and blocking opposition channels or, failing this, inventing a reason to block the service in Russia.[43]

Having no access to encrypted users' correspondence, the authorities obviously are forced to avail themselves of hackers' services, resorting to hacking and phishing. The night before 11 October 2016, Google and Yandex warned dozens of Russian activists, journalists and NGO agents of attempts by 'pro-government hackers' to crack their accounts.[44] Aleksey Shlyapuzhnikov, an expert in cybersafety who collected information about the incident, suggested that several hundreds of accounts in total could have been subject to attack.[45]

We note that, despite the fact that Oleg Kozlovsky, an opposition activist, made a statement to the authorities concerning the hack of his Telegram account[46] in May 2016, there has been no decision made whether to initiate criminal proceedings, no inquiry has been undertaken. This indirectly confirms the involvement of Russian authorities in the attack.

Conclusion

The existing system of control over Russian citizens includes a system for registration at the place of stay or residence, monitoring movement, electronic tracking, wiretapping and control of correspondence, maintaining various registers and databases for prophylactic registration of certain categories of persons, administrative supervision and so on.

Clearly criminal methods are also used here. For instance, on 23 May 2016, Grigoriy Melkonyants, co-chair of the Golos Movement for Defence of Voters' Rights, reported that his suspicions had been confirmed: the NTV TV channel had received data from wiretaps on members of his organisation from the security services: 'We decided to verify whether our curators from the security services and

[41] Protected Swiss messenger Threema denies cooperation with Russian authorities. Link: https://rublacklist.net/28518/

[42] Andrey Frolov. Durov's dialogue with the authorities. Link: https://vc.ru/p/durov-vs-zharov

[43] State massive attack against Durov: The authorities pave the way to blocking Telegram in Russia. Link: https://rublacklist.net/29749/

[44] https://www.facebook.com/kozlovsky/posts/10210285403641770?pnref=story

[45] Russian journalists and activists told about attempts of cracking their emails. Link: https://tvrain.ru/news/vzlom-418785/

[46] Opposition's SMS-service was unlocked during cracking their Telegram. Link: http://bit.ly/2tDK0HA

NTV cooperated and, to this end, we arranged a meeting today with Canadians who had contacted Roman [Udot, co-chair of GOLOS] to request such a meeting. And what happened? We caught them: NTV swallowed the bait and visited us'.[47]

Criminal proceedings are being conducted in the town of Naberezhnye Chelny**,** Tatarstan, against police officers who, *inter alia*, are accused of organising illegal surveillance in 2016-2017 of lawyers whose office was later set on fire.[48]

In June 2016 the online resource Fontanka.ru reported that journalists Denis Korotkov, Andrey Konstantinov, Evgeniy Vishenkov and Alexander Gorshkov, associates from the Agency for Journalistic Investigations working in Saint Petersburg, had been subject to surveillance operations. According to Fontanka.ru, surveillance could be related to publications regarding the activity of the businessman Evgeniy Prigozhin, the 'troll factory' from Olgino, and the involvement of a private military company in the special operation in Syria.[49]

At the same time, the Russian BBC Office suggested that the website *whoiswhos.me*, where personal data (addresses, passport details, photos, etc.) of activists, journalists and opposition politicians was published, was also supported by people from Prigozhin's circle.[50] In general, records about more than 800 people were put on the website. Shortly before that, *Novaya Gazeta* reported of a number of attacks against civic activists and bloggers whose data was also published on the website.[51]

On 4 September 2016, in Beslan (North Ossetia), an attack was made against Elena Kostyuchenko and Diana Khachatryan, journalists from *Novaya Gazeta* and *Takiye dela* who arrived there to cover commemorations events. Unknown people splashed Kostyuchenko with brilliant green dye, pulled the journalists' phones from their hands, and ran away. Prior to the flight to Moscow, the investigator gave them back the phones which allegedly were some dozens of metres away from the place of attack; all records in the phones were completely deleted.[52] As a rule, no investigation is undertaken in case of such attacks.

Despite the legal grounds provided for collecting information about virtually all residents in the country, there is much evidence of the technical and financial inability of authorities to collect, store and, moreover, process such information in a qualitative manner. The realisation of this fact incited them to decide on more thorough collection and processing of information with respect to certain groups of people. The authors of this report link this mainly with the aberration of the Russian law enforcement and control authorities to any type of 'black lists' and, in general, to delegating powers of control, surveillance and completing relevant databases of non-governmental subjects: mobile communication operators and Internet providers,

[47] Link: https://www.facebook.com/grigory.melkonyants/posts/1003159986387972

[48] MoI Lieutenant-Colonel suspected 'of all serious offences': 'I am disappointed with our law enforcement system'. Link: http://bit.ly/2ucV91o

[49] Hell's Kitchen. Link: http://www.fontanka.ru/2016/06/21/049/

[50] Andrey Soshnikov. Who is behind the Saint Petersburg 'avengers'? Link: http://bbc.in/2eMExvs

[51] Alexandra Garmazhapova, Natalia Zotova. The network over the city. Link: http://bit.ly/2vHOEpo

[52] Phones were taken away from journalists covering memorials in Beslan and all data was deleted. Link: http://theins.ru/news/29518

banks, transport companies, educational organisation; to those who, on the one hand, have access to the relevant information and, on the other hand, are strongly dependent on the State because they subsist on budgetary funds, or because of the need to obtain a license, authorisation, access to markets.

The best illustration of this appears to be the abovementioned Yarovaya packet. Within a context of economic crisis, the authorities obviously are not ready to incur the large costs needed for the implementation of a whole set of measures related to electronic tracking of citizens, which – according to different assessments – amount to RUB 130 billion[53] up to RUB 10 trillion.[54] As a result, the duties of collecting and storing the traffic data have been delegated to communications and Internet service providers, which are not happy with such a 'gift' either and have already set out to increase the prices of their services.[55] This means that citizens are actually offered to pay themselves for the possibility of the security services to read their correspondence and to review their photos: sort of paying a 'surveillance tax'. Moreover, since nowadays more than a half of the global Internet traffic is encrypted, the authorities, without having access to exabytes of users' correspondence, are forced to require from service providers to provide them with 'encryption keys'.[56]

Being aware of the limited resources, the state has oriented itself towards more thorough work with specific groups of people. Moreover, the authorities are ready to renounce some lists which failed to ensure the expected efficiency, as in the case, for instance, of the register of bloggers.

All this allows to focus the resources on different 'risk groups' that include, if needed, persons of certain interest, and to keep the population in general under control. The existence of such 'black lists' *per se* borders on violation of constitutional rights, above all, the presumption of innocence, and the prohibition of discrimination.

As a result, the security services in the numerous commercial entities consisting, as a rule, of former law enforcement agents, transfer data about their associates and customers to officials from the power structures; the management directs teachers to collect information about students or Internet providers to track users' traffic. A good illustration in this regard is a story described by Denis Karagodin of the town of Tomsk: a representative of his Internet provider asked him to provide access to his home network equipment so that to 'make diagnostics and recommend him antivirus software'. As it turned out however, the provider was perplexed by the circumstance that Karagodin accessed Internet through VPN and therefore his outgoing data flow was encrypted.[57]

---

[53] https://www.kommersant.ru/doc/3314334

[54] https://www.kommersant.ru/doc/3199479

[55] https://republic.ru/posts/70151

[56] https://tcinet.ru/press-centre/technology-news/4359/

[57] How the provider was perplexed by user's encrypted traffic. [RosComSvoboda. 2 August 2017] // https://rublacklist.net/30879/

In addition, the Russian authorities, as they collect and store an increasing volume of data about citizens, are little interested in their safety. As a result, situations in which users' data is exposed to open access are increasingly common. For instance, in May 2016 the personal data of motor vehicle owners were published on Internet,[58] and in July 2017 a department of the Russian Pension Fund sent out the personal data of almost 18,000 people via open distribution.[59]

It is not uncommon for data of certain people, mainly political activists, popular bloggers and journalists to be intentionally transferred to representatives of informal power structures or state media. In the case of the former, the aim is to conduct intimidating raids, and in the latter to shoot propaganda coverage. Members of the Pussy Riot group, the politician Aleksei Navalny, employees of the Anticorruption Fund, the popular blogger Ilya Varlamov, the journalists Diana Khachatryan and Elena Kostyuchenko, the Golos Movement for Defence of Voters' Rights, and Komanda 29 (Team 29) have all been subject to these attacks at various times.

Damir GAINUTDINOV
Legal analyst in the International Human Rights Group Agora, PhD

Pavel CHIKOV
Head of the International Human Rights Group Agora, PhD

[58] Alina Raspopova, Danila Lomakin. A crime is being investigated in the database of motor vehicle owners. Link: http://bit.ly/2huKleh

[59] Andrey Frolov. A department of the Pension Fund sent out the personal data of more than 17,000 people. Link: https://vc.ru/n/pensionfund-mistake

Agora International Human Rights Group is an association of dozens of legal professionals specialising in the legal protection of civil freedoms in the post-Soviet environment.