REPORTER OHNE GRENZEN

DIGITAL SURVEILLANCE OF CIVIL SOCIETY

by the state in Russia as well as in exile

TABLE OF CONTENTS / INHALTSANGABE

OVERVIEW OF THE LEGAL BASIS REGARDING DIGITAL SURVEILLANCE / ÜBERSICHT DER RECHTLICHEN GRUNDLAGEN BEZÜGLICH DIGITALER ÜBERWACHUNG

Zusammenfassung auf Deutsch:

Nach dem Beginn des russischen Angriffskrieges gegen die Ukraine im Jahr 2022 und seit der Annexion der Krim 2014 wurden die rechtlichen Grundlagen für die digitale Überwachung oppositioneller und kremlkritischer Bürgerinnen und Bürgern durch den russischen Staat ausgeweitet. Diese Überwachung trägt dazu bei, dass zahlreiche Grund- und Menschenrechte wie das Recht auf Meinungsfreiheit und Informationsfreiheit regimekritischer Personen und Medienschaffender sowie der Zivilgesellschaft insgesamt erheblich eingeschränkt werden.

Der folgende Textabschnitt stellt eine chronologische Auflistung rechtlicher Einschränkungen der Internetfreiheit durch erweiterte Überwachungsmaßnahmen dar. Zudem wird die technische Umsetzung digitaler Überwachung beschrieben. Die Gesetzesänderungen beinhalten unter anderem das Speichern und Teilen persönlicher und biometrischer Daten, das Unterbinden der Möglichkeit, soziale Medien anonym zu nutzen, sowie Verbote und Einschränkungen von VPN-Diensten zur Umgehung von Online-Zensur.

Although Article 29 of the Russian Constitution guarantees freedom of speech and freedom of the press and Article 23 guarantees respect to privacy, widespread evidence shows that these fundamental rights are seriously jeopardized. Over the past ten years, the respect for freedom of information and the situation of Internet regulation in Russia have been gradually deteriorating. By the time of the full-scale invasion of Ukraine, all restrictive legislative instruments had already been developed and have been widely used. Indeed, the scope for human rights in general, including privacy and personal data protection, as well as freedom of information, has been rapidly shrinking during the last few years when the **Russian government has enacted a series of restrictive laws and pursued policies that gravely violate the right to freedom of expression, digital rights and privacy, particularly targeting political opposition, civil society and journalists**. It is no surprise that a major feature of the attack on freedom of expression, digital rights and privacy has involved digital communications, and specifically the Internet, given their increasingly dominant role in modern communications. The new legislative initiatives and regulations restricting freedom of expression and Internet freedom are mainly aimed at strengthening governmental control over the media, civil society, business and primarily critics of the regime, by setting up a system of state control over the Internet and online services.

The following is a chronological list of the legal basis regarding digital surveillance which has been set in Russia over the last ten years:

1. Amendments to the Federal Law „On Personal Data Protection" entered into force in September 2015[1]. The „data localisation law" requires the personal data of Russian citizens to be stored on database servers located within Russia. Aiming at international companies who face blocking for non-compliance, the legislation is intended to enable Russian security services access to sensitive data on Russian Internet users, including activists, political opposition and journalists. The first company whose online service was blocked in Russia on this grounds was LinkedIn (since November 2016).
2. In 2017 a new set of laws was adopted, further undermining online privacy and restricting users' rights to anonymous expression:

   a. Federal Law 241-FZ,[2] which entered into force in January 2018, bans anonymity for users of online messaging applications, requiring the companies to identify users by their mobile phone numbers.

   b. Federal Law 276-FZ,[3] which entered into force in November 2017, bans Virtual Private Networks and Internet anonymizers from providing access to websites banned in Russia, and enables *Roskomnadzor*[4] to block any site explaining how to use these services.
3. A further set of amendments, called „Yarovaya Laws", which were adopted on 6 July 2016, consisting of two Federal Laws amending 19 existing laws, entered into force in 2018.[5] Justified on the grounds of „countering extremism", the amendments are broadly framed and allow arbitrary application, severely undermining the rights to freedom of expression, privacy and freedom of religion or belief.
4. The law on the digital register of the county's population was adopted in 2020, Federal Law No. 168-FZ of 08.06.2020, „On a unified federal information register containing data on the population of the Russian Federation" (on „population digital register")[6].
5. In 2021, Federal Law dated 30.12.2021 No. 441-FZ „On Amendments to Article 15-3 of the Federal Law ‚On Information, Information Technologies and Information Security' and Articles 3 and 5 of the Federal Law ‚On Amendments to Individual Statutory Acts of the Russian

1 Federal Law of 18 July 2011, No. 242-FZ On Amendments to Certain Legislative Acts of the Russian Federation for Clarification of Personal Data Processing in Information and Telecommunication Networks. Available at: www.consultant.ru/document/cons_doc_LAW_116983/

2 Federal Law of 29 July 2017, No. 241-FZ On the introduction of amendments to Articles 10.1 and 15.4 of the Federal Law On Information, Information Technologies and the defense of Information. Available at: www.consultant.ru/document/cons_doc_LAW_221183

3 Federal Law of 29 July 2017, No. 276-FZ On Amendments to the Federal Law 4 On Information, Information Technologies and Data Protection. Available at: https://cloud.consultant.ru/cloud/cgi/online.cgi?req=doc&ts=wuyGMcTcPzbxSSGi1&cacheid=99418285A7ADDE58339599B7E63DE7FD&mode=splus&rnd=lq6s5w&base=LAW&n=221230#cjtKMcTlAnQ2Wy0T

4 The Federal Service for Supervision of Communications, Information Technology and Mass Media, https://en.wikipedia.org/wiki/Roskomnadzor.

5 Federal Law of 6 July 2016, No. 374-FZ On Making Changes to the Federal Law on Counteracting Terrorism and Separate Legal Acts of the Russian Federation in Part by Establishing Additional Measures on Counteracting Terrorism and Ensuring Public Safety. Available at: www.consultant.ru/document/cons_doc_LAW_201078.

6 Federal Law No. 168-FZ of 08.06.2020 „On a unified federal information register containing data on the population of the Russian Federation". Available at: https://base.garant.ru/74232857. See the Chapter below Facial recognition technology in Russia.

Federation“ (on assigning the „unified biometric system“ status of the State information system)[7] were amended. These laws allow a unified biometric system to the level of an all-Russia state information system where biometric information, collected and stored by different governmental institutions, would be accessible to all other state bodies without notifying the individuals concerned.

6. On 14th April 2023 a very recent state legislative initiative was passed and adopted by Parliament, the Federal Law No. 127-FZ of 14.04.2023 „On Amendments to Certain Legislative Acts of the Russian Federation“[8], which introduces a new system of digital summonses to the military service and the unified register of persons subject to military mobilization.

7 Federal Law of December 30, 2021, No. 441-FZ On Amendments to Article 15-3 of the Federal Law „On Information, Information Technologies and Information Security“ and Articles 3 and 5 of the Federal Law „On Amendments to Individual Statutory Acts of the Russian Federation“. Available at: www.consultant.ru/document/cons_doc_LAW_405341.

8 Federal Law of April 14, 2023, No. 127-FZ „On Amending Certain Legislative Acts of the Russian Federation. Available at: www.consultant.ru/document/cons_doc_LAW_444711.

THE WIRETAPPING SYSTEM SORM / DAS ABHÖRSYSTEM SORM

Zusammenfassung auf Deutsch:

Das Abhörsystem SORM (System für operative Ermittlungsmaßnahmen) existiert bereits seit den 1990er Jahren als Basis für die staatliche – und insbesondere geheimdienstliche – Überwachung weit gefasster Kategorien oppositioneller Personen. Jegliche schriftliche oder mündliche Kommunikation, die über einen russischen Internet Service Provider läuft, kann im Rahmen „operativer Ermittlungsmaßnahmen" überwacht werden. Vor allem einer digitalen SORM-Überwachung durch den Geheimdienst FSB stehen keine effektiven rechtlichen Mechanismen im Wege, da jeglicher Eingriff mit dem Verdacht auf Terrorismus oder Ähnliches gerechtfertigt werden kann. Obwohl das EGMR-Urteil „Sacharow vs. Russland" vom 05.12.2015 das bestehende SORM-System scharf kritisierte, wurde dieses nach der Verkündung des Urteils mit dem restriktiven „Jarowaja-Gesetzespaket" im Juli 2016 noch weiter ausgebaut und verschärft – anstelle einer gebotenen Einschränkung.

SORM (System for Operational Investigative Measures) has existed in Russia since the 1990s. It allows the state to control wiretapping of mobile devices and other communication channels, and requires Internet Service Providers to install equipment directing all Internet traffic to a terminal within the Federal Security Service (FSB), enabling it to monitor all Internet activity, including digital private communication.9 According to Article 23 of the Russian Constitution, any restriction of the right to communicate, including direct wiretapping of private telephone communications and other correspondence, is permitted only with court authorisation and, even in these individual cases, such interference cannot amount to full access to the entire telephone or Internet correspondence. Nevertheless, FSB officers have direct access to any digital information through local control centers which represent a high risk of abuse. Moreover, SORM does not require FSB officers to present a court order to Internet Service Providers (ISPs) before accessing such information.

The operation of SORM was regulated by law, adopted to provide the authorities with details for the execution of federal laws. This was criticized, among others, in the decision of the European Court of Human Rights in the case of *Roman Zakharov v. Russia*.

The Court noted, in particular:

"The Court concludes that Russian legal provisions governing interceptions of communications do not provide for adequate and effective guarantees against arbitrariness and the risk of abuse which is inherent in any system of secret surveillance, and which is particularly high in a system where

9 See Center for Strategic and International Studies Reference Note on Russian Communications Surveillance, 18 April 2014. Available at: http://csis.org/publication/reference-note-russian-communications-surveillance.

the secret services and the police have direct access, by technical means, to all mobile-telephone communications. In particular, the circumstances in which public authorities are empowered to resort to secret surveillance measures are not defined with sufficient clarity. Provisions on discontinuation of secret surveillance measures do not provide sufficient guarantees against arbitrary interference. Domestic law permits automatic storage of clearly irrelevant data and is not sufficiently clear as to the circumstances in which the intercept material will be stored and destroyed after the end of a trial. The authorisation procedures are not capable of ensuring that secret surveillance measures are ordered only when „necessary in a democratic society."[10]

Today there are four generations of SORM:

- **SORM1** – „eavesdropping" of voice „on the fly"
- **SORM2** – „wiretapping" of traffic „on the fly" and its storage in a ring buffer for 12 hours
- **SORM3** – storage of personal data of all subscribers, storage of connection and payment statistics, metadata storage by sessions
- **SORM4** – storage of traffic content

Before starting the procedure, the FSB needs to get permission from a court for wiretapping correspondence. However, in urgent cases or those classified as serious or especially serious crimes (for example, a terrorist act), the special services can access phone calls and read messages without prior court authorization. However, the FSB agents are subsequently obliged to notify the court about these measures within 24 hours. If the court does not approve the wiretapping of correspondence, the special services are obliged to terminate their surveillance procedures, but only after receiving the written court ban. However, even if individuals were wiretapped without being charged with a crime, they will never find out or be told about it. At the moment, there are no judicial or prosecutorial oversight mechanisms of the FSB's wiretapping and interception activities.

Ignoring the strong position of the European court in the *Roman Zakharov* case, the Russian authorities, instead of repealing SORM, adopted the „Yarovaya laws", which strengthened SORM and the ability of security services to surveil peoples' private exchange of information.

10 Case of Roman Zakharov v. Russia, Application No. 47143/06, 05.12.2015. Available at: https://hudoc.echr.coe.int/eng?i=001-159324.

THE „YAROVAYA LAWS“: „ORGANIZERS OF INFORMATION DISTRIBUTION“ (OID) / DAS „JAROWAJA-GESETZESPAKET”: DIENSTE DER INFORMATIONSVERBREITUNG

Legal basis and the general situation / Rechtslage und Allgemeines

Zusammenfassung auf Deutsch:

Seit Juli 2016 wurde es durch die Verabschiedung des „Jarowaja-Gesetzespakets“ für den Staat rechtlich möglich, beim Vorliegen „berechtigter Interessen der Staatssicherheit“ nicht nur schriftliche und mündliche Kommunikation über in Russland registrierte Internet Provider engmaschig zu überwachen, sondern auch den Schutz des Briefgeheimnis seitdem de facto auszuhebeln. Diese Gesetzesänderungen vom Juli 2016 eröffneten den Weg für eine Ausweitung digitaler Überwachung für alle russischen Behörden, die berechtigt sind, „operative staatliche Maßnahmen“ durchzuführen. Dies betrifft den Geheimdienst FSB, alle Strafverfolgungs- und Ermittlungsbehörden, darunter die Polizei, den Föderalen Strafvollzugsdienst sowie den Föderalen Zolldienst. Der angepassten Rechtslage zufolge wurde digitale Überwachung sogar bei jeglicher WiFi-Nutzung in Russland möglich, da sich auch alle WiFi-Provider in Russland anmelden müssen.

Mehrere staatliche Stellen sind an der direkten Kontrolle der Kommunikation und Meinungsäußerung im Internet beteiligt, leisten gleichzeitig aber auch unterstützende Maßnahmen für russische Strafverfolgungsbehörden. Die Hauptakteure sind die staatliche Medienaufsichtsbehörde Roskomnadsor und die Abteilung des Innenministeriums zur Bekämpfung von Extremismus (das so genannte Zentrum „E“ der Polizei). Sie überwachen Online-Beiträge, soziale Medien, Online-Medien, machen Screenshots oder dokumentieren in einer anderen Form Äußerungen und Veröffentlichungen im Internet, die künftig als Begründung für die Anklage von Personen aufgrund einer breiten Palette von Straftaten dienen können. Darunter fallen inhaltliche Einschränkungen wie „Fakenews“, Diskreditierung der Streitkräfte bis hin zu Extremismus, Rechtfertigung von Terrorismus, und so weiter.

Die Überwachungsmaßnahmen von Roskomnadsor und dem Zentrum „E“ beziehen sich auf „rechtswidrige“ Aktivitäten im Internet und müssen somit keinen geografischen Bezug ausschließlich auf in Russland befindliche Personen haben. Bekannte Fälle zeugen davon, dass auch im Exil lebende Personen digital überwacht wurden. Seit dem 24.02.2022 wurden gegen russische Medienschaffende Dutzende Strafverfahren wegen des Verbreitens von „Fakenews“ und „Diskreditierung der Streitkräfte“ eingeleitet als sie sich bereits im Exil befanden (wie zum Beispiel Dmitrij Kolesew, Chefredakteur von „Republic Media“). Auch die Anhänger von Alexej Nawalny wurden in den vergangenen Jahren gezielt überwacht und strafrechtlich über die Staatsgrenzen hinaus verfolgt.

Das vorliegende Kapitel beantwortet darüber hinaus die Frage, ob und in welchem Umfang bei Protesten überwacht wird. Ebenso wird die Verbindung von Protesten auf der Straße und anschließender oder sogar vorbeugender digitaler Überwachung über soziale Medien hergestellt.

The „Yarovaya laws"[11] (or „Yarovaya package") were submitted for consideration to the State Duma by Irina Yarovaya, a Member of Parliament and Chair of the Duma Security Committee. The „Yarovaya laws" comprise two laws[12] introducing a number of amendments to nineteen Federal laws, namely the

- Federal Law on „Countering Terrorism";
- Federal Law on „Federal Security Service";
- Federal Law on „Operation-Search Activity";
- Federal Law on „Foreign Intelligence";
- Federal Law on „Arms";
- Criminal Code;
- Criminal Procedure Code;
- Air Code;
- Federal Law on „Freedom of Conscience and Religious Associations";
- Federal Law on „Postal Communication";
- Federal Law on „Countering the Legalization (Laundering) of Criminal Income and the Financing of Terrorism";
- Code of Administrative Offences;
- Federal Law on „Transportation and Expeditionary Activity";
- Federal Law on „Communications";
- Housing Code;
- Federal Law on "Information, Information Technologies and Data Protection";
- Federal Law on „Transport Security";
- Federal Law on „Territorial Jurisdiction of the District (Naval) Military Courts";
- Federal Law on „Safety of Fuel and Energy Complex".

11 Federal Law On Amendments to the Federal Law 9 On Countering Terrorism and certain legislative acts of the Russian Federation regarding the establishment of additional measures to counter terrorism and public safety of 6 July 2016, No. 374-FZ, and Federal Law On Amendments to the Criminal Code of the Russian Federation and the Code of Criminal Procedure of the Russian Federation regarding the establishment of additional measures to counter terrorism and ensure public safety of 6 July 2016, No. 375-FZ.

12 Federal Law On Amendments to the Federal Law 9 On Countering Terrorism and certain legislative acts of the Russian Federation regarding the establishment of additional measures to counter terrorism and public safety of 6 July 2016, No. 374-FZ, and Federal Law On Amendments to the Criminal Code of the Russian Federation and the Code of Criminal Procedure of the Russian Federation regarding the establishment of additional measures to counter terrorism and ensure public safety of 6 July 2016, No. 375-FZ.

These amendments introduced new forms of control over private correspondence and online activity. They also, through legislation, impose detailed rules on what kind of content needs to be retained by telecom operators including ISPs and for what period of time, impose additional restrictions on citizens and operators, and expand the powers of law enforcement agencies in the context of operational investigation activities.

With the adoption of the „Yarovaya laws", in the framework of operational investigations, law enforcement agencies now have the right to exert *„control over mail, telegraph and other messages, listen to telephone conversations with connection to the station equipment of enterprises, individuals … providing services and means of communication"*[13], all without special judicial authorization as long as they consider that access to such information is justified by the interests of „state security". At the same time, the concept of „state security" is interpreted very broadly and is actively used by the authorities to restrict the rights and legitimate interests of citizens, including in the framework of law enforcement in practice. This makes the „Yarovaya laws" arbitrary in terms of implementation as well as restrictive in terms of privacy and freedom of expression.

Justified on the grounds of „countering extremism", the „Yarovaya laws" are broadly framed, allowing for arbitrary application and severely undermining the rights to freedom of expression, privacy and freedom of religion or belief. Although the „Yarovaya laws" were justified on the basis of countering terrorism, they also include substantial additional restrictions on privacy and communications rights and freedoms of citizens of Russia, including through the creation of a system of control over people's correspondence. The excessive and unreasonable interference by the state into citizens' private life inevitably creates an atmosphere of self-censorship for online discussions and **even in private correspondence and telephone conversations, limiting the free exchange of opinions, creating legal risks of prosecution**.

Operators are required to store extensive communication data. A violation of this requirement leads to administrative liability, through amendments to the laws „On Communications", „On Information, Information Technologies and Data Protection" and the Code of Administrative Offenses.

The „Yarovaya laws" apply to the communication data of Internet and mobile communication users with Russian IP addresses or who have a Russian cell phone number or Russian passport. Also, operators are obliged to keep the correspondence of foreigners who, according to the Ministry of Internal Affairs, are on Russian territory. All of this metadata and communication data (text messages, voice information, images, sounds, video and other electronic messages) must be stored by Organizers of Information Distribution (OID) between 6 to 36 months provided a request is issued by the security service FSB and any other law enforcement body, which is legally entitled to conduct operational search activities (i.e. pre-investigation activities), including the police, Federal Penitentiary Service, Federal Customs Service and foreign intelligence service.[14] These instruments are equipping law enforcement bodies, as well as supporting activities by these bodies, to control communication online.

Furthermore, the „Yarovaya laws" require operators to identify their subscribers by their mobile phone number, which in turn is registered to the user with his or her passport details.[15] This information, in turn, is used by the special services in order to determine the exact identity of people engaged in certain conversations and correspondence. This seriously undermines the right to anonymity of Internet users, since any connection to a public wifi network in Russia will now take place only once

13 Article 6(4) of the Federal Law On Operational Search Activity and Article 1.1 of the Federal Law On Communication.

14 Article 64(1.1) of the Federal Law On Communications of 7 July 2003, No. 126-FZ.

15 Article 64(1.1) of the Federal Law On Communications and Article 13.20 of the Code of Administrative Offenses.

a user is identified. At the same time, the provisions of the „Yarovaya laws" oblige operators to stop providing services to a subscriber if law enforcement bodies carrying out criminal investigations request the subscriber's identity and the operator cannot confirm this within 15 days.[16]

In addition to that, a few governmental bodies are actively involved in monitoring and controlling online communication and expression. Reports issued by these governmental bodies are widely used as evidence in administrative and criminal cases against perceived and real opponents and dissidents. The two main state bodies conducting such „online" investigative activities are the State Media Regulator *(Roskomnadzor)* and the Ministry of Interior (Police) department on counteracting extremism (the so-called „Centre E"). These two bodies are closely monitoring publications online, social media, online media, and use screenshots and other forms of documentation which are used as grounds for charging people for all sorts of offenses (ranging from content restrictions like „fake news" and discreditation of armed forces to extremism and justification of terrorism – as was the case of journalist Svetlana Prokopieva[17] or the civilian Ekaterina Muranova[18], and many others – and even treason – as was the case of Vladimir Kara-Mursa who was sentenced in 2023 to 25 years of imprisonment). These bodies are responsible for the close monitoring of the Internet, as one of their main activities within their scope of jurisdiction and powers.

According to public reports and case law, supporters of Alexey Navalny and his political activities (via the Anti-Corruption Foundation (FBK) and networks of Navalny regional headquarters) were under specific monitoring and prosecution campaigns during the last few years, many of them having been charged for extremist activity and ultimately resulting in the FBK being declared an extremism organization in June 2021. During massive anti-corruption protests in 2017, following the release of the anti-corruption film „He is not Dimon", dedicated to Dmitry Medvedev, a high number of people were detained during the crackdown on protests. **This was followed by a specific surveillance campaign in the Russian social media network VK („VKontakte") which focused on high school students aged between 15 and 18 years who were following Alexey Navalny and FBK activities and who were part of Navalny's VK public groups.** Police interrogated students and had „talks" with their parents on the anti-state purpose of Navalny's activity. They also threatened students with possible punishment for participating and for just being members of his VK public groups (i.e. just for reading the content).

The same monitoring activities by state control bodies is being conducted now and probably on a much higher scale. **Social media and public expression online, when written in Russian language, even if the Russian citizen is not located in Russia, are equally monitored, because these publications are accessible to Russian audiences and can influence public opinion. This is the reason why there is such a high number of blocked online media, in particular since February 2022.**

Over a dozen criminal cases have been initiated against Russian journalists for war-related expressions and war coverage, even though these journalists were not in Russia at the time of publication and were publishing their materials working from a different country. For instance, Dmitry Kolezev, editor-in-chief of Republic media, was charged under Art. 207.3 of the Russian Penal Code for „fake news" against Russian Armed forces, declared a „foreign agent" and announced to be wanted on federal and international level.

16 Article 46 of the Federal Law On Communications.

17 Human rights center MEMORIAL, „Prokopyeva Svetlana Vladimirovna, https://memohrc.org/ru/defendants/prokopeva-svetlana-vladimirovna.

18 Current Time, www.currenttime.tv/a/ekaterina-muranova-karelia-fsb/30272175.html.

The rules noted above do not only give the state extensive access to information about the private life of citizens but also allows it to control discussions and correspondence of civil activists, human rights defenders and employees of NGOs, all on an absolutely legal basis. The arbitrary law enforcement practice which has been observed in Russia in recent years – the absence of an independent judiciary and the virtually unlimited powers of the special and security services suggest that the „Yarovaya laws", like many recent legislative initiatives as outlined in Chapter 1, are being used arbitrarily. According to the „Yarovaya laws", all those present in Russia, citizens and foreigners alike, are effectively considered as potential offenders, so much so that only total state control of all communication can ensure „state security".

Organizers of Information Distribution (OID) / Dienste der Informationsverbreitung (OID)

Zusammenfassung auf Deutsch:

Seit Mai 2015 werden alle in Russland tätigen Kommunikationsdienste, einschließlich Messengerdiensten wie Telegram, von Roskomnadsor als sogenannte „OIDs" (Dienste der Informationsverbreitung) erfasst und durch Art. 10.1 des russischen Informationsgesetzes verpflichtet, auf Anfrage des Geheimdienstes FSB auch die Sicherheitsschlüssel zu verschlüsselten Nachrichten zur Verfügung zu stellen. Bei Verweigerung drohen Sanktionen bis hin zu einer kompletten Zugangssperre zum jeweiligen Kommunikationsdienst in Russland. Eine solche Anfrage wurde im März 2018 auch an den Messengerdienst Telegram gestellt.

Zum Zeitpunkt der Verfassung dieser Stellungnahme sind 311 Kommunikationsdienstleister von Roskomnadsor als „OID" erfasst worden, unabhängig davon, ob es russische oder internationale Internetprovider sind. Im aktuellen Textabschnitt folgt eine Auflistung.

Am 13. Februar 2024 entschied der Europäische Gerichtshof für Menschenrechte im ersten Telegramm-Schlüssel-Fall, dass Russlands „Jarowaja-Paket" die Sicherheit aller Internetnutzer gefährdet. Das Fehlen rechtlicher Schutzmaßnahmen und die Möglichkeit der Geheimdienste, ohne Genehmigung direkt auf die Internetkommunikation jedes Bürgers zuzugreifen, verletzten das Recht auf Privatsphäre. Das Gericht argumentierte, dass die gesetzliche Verpflichtung zur Entschlüsselung von Ende-zu-Ende verschlüsselter Kommunikation die Verschlüsselung für alle Nutzerinnen und Nutzer nicht mehr sicher machen würde, was den legitimen Zielen widerspricht.

Another actor involved in digital surveillance is „the organizer of information distribution". According to Article 10.1 of the Law „On Information, Information Technologies and Data Protection",

"the organizer of information distribution in the Internet is a company carrying out activities to ensure the functioning of information systems and (or) programs for computers that are intended and/or used to receive, transmit, deliver and (or) process electronic messages of Internet users".

Online services which *Roskomnadzor* has declared to be OID must provide decryption keys for any encrypted messages to the security services. A failure to comply with this rule may lead to sanctions,

including blocking access to these services in Russia (as has happened with Telegram, a messaging and social networking application, in 2018, which was temporarily blocked from June 16, 2018, to June 18, 2020).[19] These companies may also only use encryption tools which have been certified in Russia. However, such certifications of encryption tools carried out by states cannot be regarded as trustworthy. These rules deny users the protection of private correspondence which is available with reliable foreign encryption and digital security tools, and threatens not only ordinary Internet users but also civil society activists and journalists (and their confidential sources of information).

The authorities, after receiving the decryption keys from the Russian manufacturers or companies that have passed certification in Russia, will be able to read the coded correspondence of any citizen and use this information in their sole discretion, including when they are conducting their work in secret.

The requirements for the storage of user information by the OID is similar to that for telecom operators. Specifically, the rules stipulate that these services must retain data about users who can be identified as being in the territory of the Russian Federation (by IP address, telephone number and geographical metadata) or as being Russian citizens (based on an identity document, even if the user is located outside of Russia). The organizer of information distribution should store full content of all electronic messages from such users for six months from the date of sending, receiving, delivering, transmitting or processing those messages, and this information shall, upon request, be provided to the approved state authorities (such as the FSB and the police). The system is called SORM-4.

At the moment of drafting this report in April 2023, the list of such organizers of information distribution (OID) contains 311 companies[20], including social networks (Russian social networks, such as vk.ru, odnoklassniki.ru), websites with forums (thematic websites and many online media providing for interaction with and between readers), online meeting services (such as tinder.com, mamba.ru), mobile applications, and other online services which provide tools for communication between users, such as vimeo.com and wechat.com. A wide range of websites which are accessible in Russia, including many foreign ones – including online stores, blogs, message services (Twitter, WhatsApp and others), social networks, online media and forums – have been technically identified as OIDs.

In the case related to the blocking of the social media channel Telegram and the demands by the Russian authorities to provide encryption keys (see also the OSCE statement[21]), at least 3 cases are pending before the ECtHR: „Podchasov against Russia“ (application no. 33696/19), „Telegram Messenger LLP and Telegram Messenger Inc. v. Russia“ (communicated case, application no. 13232/18), „Private Networks LP against Russia“ (application no. 4945/20).

On February 13, 2024, the European Court of Human Rights (ECtHR) issued its first judgment in the initial Telegram encryption key case (Anton Podchasov v. Russian Federation). Using this case as an example, the Court for the first time considered the regulation of end-to-end encryption and storage of user data of Internet services and recognized that the „Yarovaya Laws“ threatens the security of all Internet users.

The ECtHR decision in Roman Zakharov v. Russia served as a basis for considering the legal aspects of secret surveillance, recognized by the ECtHR as the same for both telecommunications operators

19 News.ru, Roskomnadzor sent Telegram a notice about the need to provide the FSB with the keys to decrypt messages (www.newsru.com/hitech/20mar2018/rkntelegram.html).

20 Online-register of banned Internet-sites (https://reestr.rublacklist.net/ru/disseminators).

21 OSCE, Blocking of Telegram and legal restrictions on social networks will limit freedom of expression in Russia, says OSCE Representative Désir, https://www.osce.org/representative-on-freedom-of-media/377767.

and disseminators of information. The ECtHR reiterated that the right to respect for private life secured by Article 8 of the European Convention on Human Rights had been violated. The absence of legal safeguards, in particular the requirement to „present a judicial authorization to the telecommunications service provider before accessing personal communications in accordance with domestic law", as well as the obligation to install technical equipment to obtain remote access to all Internet communications and related data, supported the argument that such interference was not necessary in a democratic society.

The ECtHR concluded that „the Russian legal system, which gives the intelligence services direct access to any citizen's Internet correspondence without requiring authorization for interception either from the communication provider or from anyone else, is particularly prone to abuse. After examining the provision that obliges information disseminators to decrypt data, the court found „that, in this context, a statutory duty to decrypt end-to-end encrypted communications may amount to a requirement that providers of such services weaken the encryption mechanism for all users; it is therefore inconsistent with the legitimate aims pursued." The court argued that it is technically impossible to provide discriminatory access to encrypted messages, i.e. access to certain Telegram users of interest, while Russian law provides for the opposite – unrestricted access to messages and other data of all users in an attempt to weaken encryption for all users.

DE-ANONYMIZATION ONLINE / DEANONYMISIERUNG IM INTERNETBEREICH

Zusammenfassung auf Deutsch:

Ein weiteres russisches Gesetz, Nr. 241-FZ vom Juli 2017, zielt darauf ab, die Anonymität von Medien sowie Nutzerinnen und Nutzern im Internet unmöglich zu machen. Unter anderem verbietet es anonyme Telegram-Kanäle und anonyme Kanäle in anderen Messengerdiensten, die in Russland tätig sind.

Im März 2023 wurde öffentlich bekannt, dass die Staatsgesellschaft Rostech über die sogenannte Hunter-Technologie zur Deanonymisierung verfügt, welche es ermöglicht, die Nutzeridentität anhand von Handynummern, Geolokalisierungsdaten und IP-Adressen festzustellen. Diese Technologie soll insbesondere gegen die Betreiberinnen und Betreiber anonymer Telegram-Kanäle und anonymer Bloggerinnen und Blogger verwendet werden. Es ist damit zu rechnen, dass Rostech diese Daten an russische Strafverfolgungsbehörden liefern oder verkaufen wird.

Eine investigative Untersuchung des Journalisten Andrej Sacharow vom März 2023[22] zeigte, dass die Polizei in drei russischen Regionen bereits das „Insider"-System als Teil der „Laplace Demon"-Software erworben hat, um Gruppen, Konten und Chats auf der Internetplattform VKontakte zu überwachen und Telegram-Nutzer zu deanonymisieren.

Anonymity, according to the position of the Russian authorities, is not a right of users but an evil that must be fought. The Strategy for the Development of the Information Society until 2030[23] associates online anonymity with „impunity and irresponsibility". Thus, the Russian authorities are taking consistent action to de-anonymize Internet users.

Immediately after the signing of the Strategy in July 2017, the State Duma adopted Federal Law No. 241-FZ („the law on messengers"), which imposes on owners of messengers the obligation „to identify users using a subscriber number, based on the identification agreement concluded by the organizer of instant messaging with the telecommunications operator."

In March 2023, it became known[24] that the state company Rostech bought software from the St. Petersburg-based private company T.Hunter and now owns a tool to de-anonymize the owners of anonymous channels in Telegram, which it intends to sell to law enforcement agencies. Hunter is able to identify the accounts of administrators and owners of Telegram channels using its own neural

22 The Telegram Channel of the investigative Journalist Andrei Zakharov, https://t.me/zakharovchannel/1254.

23 The official Internet portal of legal information in the Russian Federation, https://pravo.gov.ru/proxy/ips/?docbody=&nd=102431687.

24 The Bell, Rostec has learned to identify the owners of anonymous Telegram feeds and will sell this service to the law enforcement agencies, https://thebell.global.ssl.fastly.net/rostekh-budet-postavlyat-silovikam-po-dlya-deanonimizatsii-tele-kanalov.

network. The identities of channel administrators are identified by cell phone number, geolocation data and IP address.

In March 2023, the journalist Andrei Zakharov conducted[25] an investigation that claimed that police in three Russian regions have already purchased the „Insider“ system as part of the „Laplace Demon“ software to monitor groups, accounts and chats in VK and de-anonymize Telegram users.

25 Andrei Zakharov s Channel on Telegram, https://telegra.ph/Siloviki-i-chinovniki-ispolzuyut-slitye-bazy-chtoby-deanonit-polzovatelej-Telegram-Za-byudzhetnye-dengi-03-06.

FACIAL RECOGNITION TECHNOLOGY IN RUSSIA / GESICHTSERKENNUNGSTECHNOLOGIE IN RUSSLAND

Zusammenfassung auf Deutsch:

Seit Beginn 2023 wird das Gesichtserkennungssystem aktiv verwendet, um Kriegsdienstverweigerer zu identifizieren sowie „vorbeugend", um beispielsweise Proteste zu unterbinden. Seit 2018 wurden in Moskau über 250.000 CCTV-Kameras installiert. Spätestens seit 2021 werden sie von den Strafverfolgungsbehörden aktiv angewendet. In den Jahren 2021 bis 2022 registrierte die russische Menschenrechtsorganisation OVD.info, 595 Festnahmen auf Grundlage einer Videoüberwachung im öffentlichen Stadtraum.

2023 entschied das Europäische Gericht für Menschenrechte[26], dass Russlands Nutzung von Gesichtserkennungstechnologie gegen die Privatsphäre verstoße. Ein russischer Staatsbürger, Nikolai Gluchin, wurde auf der Grundlage von Fotos in sozialen Netzwerken und Überwachungsaufnahmen im Moskauer Stadtraum nach einem friedlichen Protest festgenommen. Obwohl das deklarierte Ziel russischer Sicherheitskräfte lautete, mögliche Gesetzesverstöße und Unruhen zu verhindern, gab es nach der Einschätzung des EGMR keine klaren Regeln für den Einsatz der Überwachungstechnologie. Digitale Überwachungsmaßnahmen wurden vom Gericht als unverhältnismäßig eingestuft, da der friedliche Protest keine Bedrohung darstellte. Das EGMR urteilte, dass die Verwendung der Überwachungstechnologien gegen demokratische Prinzipien verstößt.

Ende 2023 schlug das russische Ministerium für Digitalisierung die Schaffung einer landesweiten Infrastruktur vor, welche die lokalen Behörden bei der Implementierung von Gesichtserkennungssystemen unterstützen soll. Dies deutet auf eine Einführung eines föderalen Gesichtserkennungssystems hin. Zum aktuellen Zeitpunkt sind in Russland mehr als 1 Million Videokameras installiert, wobei jede dritte Kamera mit Gesichtserkennungssystemen verbunden ist.

Moscow has one of the largest video surveillance systems in Europe. Images from over 250.000 CCTV cameras throughout the capital (including entrance cameras in apartment buildings, commercial buildings, streets and transport) are fed to Moscow government servers, allowing them to process these images with the assistance of detection and identification modules and eventually identify the faces of everyone who gets caught in the lens. For this purpose, Moscow simultaneously uses four algorithms from Russian and Belarusian vendors: NtechLab, Tevian FaceSDK, VisionLabs Luna Platform and Kipod.

The facial recognition system (known as „Sphere") began operating in Moscow in 2018 during the FIFA2018 World Cup, and the need for its implementation was explained by the desire to ensure the safety of guests attending the games. Later, officials stated that the system was needed to search

26 ECHR, Glukhin vs. Russia, Application no. 11519/20, https://hudoc.echr.coe.int/?i=001-225655.

for lost people, then to ensure security during mass events (including rallies and protests). In 2020, authorities began to explain that the system was necessary to ensure public health and compliance with lockdown. **Since 2022 the facial recognition system began to be used for „preventive detentions" on state holidays or important public events, when protest activity is more likely. Most of those detained in the Moscow Metro since 2022 had been previously prosecuted for participating in protests or for discrediting the Armed Forces.** In addition, some of the detained individuals had not been prosecuted before, but had previously participated in protest rallies and **were recognized by video surveillance, or were known to be registered on opposition platforms' websites, participated in democratic forums, and so on**. As a rule, such detentions were accompanied by a delivery to a department of the Ministry of Internal Affairs and a preventive conversation. Between 2021 and 2022 OVD-Info and RoskomSvoboda recorded[27] at least 595 detentions using the facial recognition system. In 2023, the system has already been used to catch people fleeing mobilization for war. To date, numerous cases of illegal use of the technology have been documented[28], but during court hearings the authorities deny using the system to spy on citizens.

In all administrative claims against the Moscow City Interior Ministry and the Moscow City Government, the Moscow courts dismissed all applicants' claims, including the „Anna Kuznetsova case,"[29] in which facts of malpractice were previously legally established. As a result, activist Anna Kuznetsova, politician Vladimir Milov, and social activist Alyona Popova appealed to the European Court of Human Rights (ECtHR) over mass face recognition technology. The complaints are currently awaiting communication with the ECtHR.

In 2023, the ECtHR ruled in a unanimous decision in Glukhin v. Russia that the activation of online facial recognition technology without lawful procedural measures and controls violated the right to privacy protected by Article 8 of the European Convention on Human Rights. On August 23, 2019, Nikolai Glukhin, a Russian citizen and the applicant, walked through the Moscow metro with a cardboard image of Konstantin Kotov, a participant in a protest demonstration whose case caused public outrage and attracted widespread media attention, holding a sign reading „You are probably joking. I am Konstantin Kotov. I am facing up to five years under [Article] 212.1 [of the Russian Criminal Code] for peaceful protests." In the course of Internet monitoring, police discovered photos and videos of Glukhin's participation in the subway demonstration, which had been published on an open social networking website. Glukhin speculated that facial recognition technology could be used against him to identify him in screenshots from the social network and footage from CCTV cameras installed at metro stations. He was arrested a few days later, likely by using facial recognition technology to determine his presence on the subway in real time. Glukhin was later prosecuted for an administrative offense for failing to inform the authorities about his solitary picket using a „quickly (de)assembled object." He was fined 20,000 rubles (approximately 283 euros). Social media screenshots and surveillance footage from the cameras he walked through on August 23, 2019 were presented to the police as evidence against him. On October 30, 2019, the Moscow City Court upheld his conviction on appeal, finding, among other things, that the peaceful nature of the

27 Human Rights and New Technologies in Russia. Joint Submission to the UN High Commissioner, https://roskomsvoboda.org/uploads/ovd-info_and_roskomsvoboda_-_input_for_report_on_technical_standards_and_human_rights.pdf.

28 Roskomsvoboda, The campaign against facial recognition, https://bancam.ru/#history.

29 Tverskoy District Court of Moscow, case No. 02029-0798/2020, https://mos-gorsud.ru/rs/tverskoj/services/cases/kas/details/151b3db1-0400-11eb-a7b5-d914ac4c1d0c?participants=%D0%94%D0%B5%D0%BF%D0%B0%D1%80%D1%82%D0%B0%D0%BC%D0%B5%D0%BD%D1%82+%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D1%85.

demonstration in which he participated was irrelevant and that the offense had been detected and the evidence collected in accordance with the Police Act. The ECtHR observed that Glukhin had found it difficult to support his claim that facial recognition technology had been used in his case.

ECtHR noted that open sources confirmed numerous cases of the use of facial recognition technology to identify participants in protest actions in Russia. In this regard, the ECtHR concluded that the processing of Mr. Glukhin's personal data in the course of the investigation of an administrative violation, including the use of facial recognition technology to detect him and his subsequent detention, violated his right to privacy.

On the one hand, such interference has its basis in domestic law, namely the Code of Administrative Offenses and the Federal Law „On Police". These laws give the police powers to investigate administrative offenses and to collect evidence, including personal data. Thus, the purpose of the interference with Mr. Glukhin's rights was a legitimate one – to prevent an administrative violation.

On the other hand, the ECtHR pointed out that there were no specific rules in the national law that would regulate the application and scope of measures related to the use of facial recognition technology. Moreover, there were no convincing safeguards against the possibility of abuse and arbitrariness. The actions committed against Mr. Glukhin were particularly disproportionate, given that it was a peaceful protest that did not pose a threat to society or transport safety. In fact, he was prosecuted for a minor breach of the law. Thus, the processing of the applicant's biometric personal data using facial recognition technology in the course of the administrative infringement case – firstly, to determine his identity from photographs and videos posted on the internet, and secondly, to detect and arrest him while he was traveling on the Moscow metro – did not meet an „urgent public need" and could not be regarded as „necessary in a democratic society". The ECtHR characterized the measures applied to the applicant as „particularly intrusive" because they involved facial recognition technology.

In these circumstances, the Court found that the use of facial recognition technology to identify the applicant was not in accordance with an „urgent public necessity" and was incompatible with the principles and values of a democratic society based on the rule of law, which the European Convention seeks to reinforce and uphold.

Up until now, there has been no regulatory framework for biometric identification in public places without the consent of the subject; this includes the requirements for a citizen's reference image, the criteria for image matching, a closed list of the grounds for such processing (other than the general rule in Article 11 of Federal Law No. 152-FZ dated July 27, 2006 „On Personal Data"), the procedure for providing access to the system and measures for effective oversight and legal protection.

Moreover, at the end of 2023, the Ministry of Digitalization has already proposed[30] an initiative to create a nationwide basic infrastructure and toolkit for other constituent entities of the Federation that will help local authorities deploy facial recognition systems, which means a move towards a nationwide federal facial recognition system. The total number of video cameras in Russia today is more than 1 million. At the same time, every third video surveillance camera is connected to facial recognition systems.

30 www.rbc.ru/technology_and_media/24/11/2023/65604ba09a7947eb3df38cf7.

TARGETING RUSSIAN JOURNALISTS IN EXILE WITH PEGASUS SPYWARE / ÜBERWACHUNG RUSSISCHER MEDIENSCHAFFENDER IM EXIL MIT DEM PEGASUS STAATSTROJANER

Zusammenfassung auf Deutsch:

2021 enthüllten internationale Recherchen rund um das „Pegasus-Projekt" erstmals das Ausmaß der staatlichen Überwachung durch Staatstrojaner der israelischen Firma NSO Group. Die Schadsoftware erlaubt Angreifenden den nahezu grenzenlosen und heimlichen Zugriff auf sämtliche Daten infizierter Geräte. Darüber hinaus können Kamera- und Sprachfunktionen des Telefons aktiviert und ohne Wissen der Nutzenden Aufnahmen gemacht werden. Im September 2023 veröffentlichten das Citizen Lab und Access Now einen Bericht, der erstmals den Angriff auf eine russische Exiljournalistin belegte. Aus dem Bericht geht hervor, dass die Herausgeberin der russischen, unabhängigen Nachrichtenseite Meduza, Galina Timtschenko, während eines Aufenthalts in Berlin mit der Spähsoftware Pegasus überwacht wurde. Demnach wurde ihr Smartphone um den 10. Februar 2023 infiziert, zwei Wochen nachdem die russische Regierung Meduza wegen ihrer kritischen Berichterstattung über den Krieg gegen die Ukraine zu einer „unerwünschten Organisation" erklärt hatte. In der Folge dieser Enthüllungen berichteten drei weitere in Lettland ansässige Journalist*innen, dass Apple sie darüber informiert habe, dass ihr Telefon womöglich Ziel eines ähnlichen Hackerangriffs gewesen sein könnte.

Digital surveillance puts not only journalists at high risk but also endangers their journalistic sources at a large scale. It is a method oftentimes used to intimidate and silence individuals with the aim to suppress critical public reporting. A report published on 13 September 2023 by Access Now and the Citizen Lab has revealed that the Pegasus spyware was used to spy on Galina Timchenko, Russian journalist and publisher of the independent news website Meduza.[31] Spyware like NSO Group's Pegasus abuses vulnerabilities in devices to be installed without the consent of targeted individuals. It enables perpetrators to access all data stored on mobile devices, to listen in and record conversations in real-time by secretly switching on microphones as well as the camera of any infected phone. According to the published report, Timchenko's smartphone was infected with Pegasus on or around 10 February 2023, when she was in Berlin for meetings. This first-time use of Pegasus against Russian journalists in exile came just two weeks after the Russian government declared Meduza an „undesirable organization" for their critical coverage of the war in Ukraine. In the aftermath, three other Latvia-based journalists

31 Access Now, www.accessnow.org/publication/hacking-meduza-pegasus-spyware-used-to-target-putins-critic

reported that Apple had notified them that their phone could have been targeted by such hacker attacks.[32]

One of the main problems with spyware like Pegasus which is sold to governments and their agencies all around the world is that these tools are extremely sophisticated and powerful. At the same time they are made to obfuscate the perpetrator, making it hard to identify those behind the attacks. In the case of Galina Timchenko, Access Now and the Citizen Lab listed three hypotheses about the possible origin of the hacking attack: according to the first hypothesis, Germany, Estonia and Latvia could be potential suspects as these states acquired Pegasus; the second possibility holds responsible the states allied with Russia, such as Azerbaijan, Kazakhstan or Uzbekistan that are also known to be Pegasus customers, although attacks against individuals living in the EU have never been observed so far.[33] The third hypothesis states that Russia itself could be responsible for the espionage, however, there are currently no indications that Pegasus was sold to the Russian state. Because the installation of spyware is difficult to detect or prove, the mere suspicion that spyware could have been installed leads to massive uncertainty and reticence among Russian journalists in exile.

32 CPJ, https://cpj.org/2023/09/apple-warns-latvia-based-journalists-about-possible-hacker-attacks.

33 Amnesty International, www.amnesty.org/en/latest/news/2023/05/armenia-azerbaijan-pegasus-spyware-targeted-armenian-public-figures-amid-conflict.

UNIFIED STATE REGISTERS OF RUSSIAN NATIONALS' PERSONAL DATA / EINHEITLICHE STAATLICHE REGISTER MIT PERSONENBEZOGENEN DATEN RUSSISCHER STAATSANGEHÖRIGER

Zusammenfassung auf Deutsch:

Seit Juni 2020 (implementiert seit Beginn 2023) erfasst der Föderale Steuerdienst (FNS) personenbezogene Daten aller russischen Staatsangehörigen. Es ist nicht ausgeschlossen, dass diese Daten im Rekrutierungsverfahren für den Kriegsdienst Verwendung finden werden. Das Föderale Gesetz Nr. 127-FZ vom 15. April 2023 ermöglicht eine formelle „Zustellung" des Einberufungsbescheids nach einer in diesem Gesetz bestimmten Frist allein durch ihre Veröffentlichung im elektronischen Register, was für alle wehrpflichtigen Personen russischer Staatsangehörigkeit (überwiegend Männer) zwischen 18 und 60 gilt.

The Russian authorities continue to collect data on every inhabitant of the country. In June 2020, Federal Law No. 168-FZ „On the Unified Federal Information Register Containing Data on the Population of the Russian Federation" was enacted. The main provisions of the law came into force in 2023. „The Unified Population Register" (UPR) is designed to bring together data about each person from a multitude of agencies. Its operator is the Federal Tax Service (FTS). One of the drafters of this law comments on it as follows: „Bringing all information systems to one denominator will give birth to the so-called ‚golden ideal profile', which will summarize approximately 30 types of information from 12 major providers".

On April 15, 2023, President Putin signed Federal Law No. 127-FZ „On Digital Military Summonses". In addition to establishing in the law that a military subpoena is considered served to a citizen after 7 days from the moment of its placement in the register of digital summonses, the law also provides for the creation of a Unified Digital Register of citizens subject to mobilization. All state bodies and courts, medical organizations, private companies and universities will be obliged to transfer data to this registry.

ILLEGAL PROFILING / ILLEGALES PROFILING

Zusammenfassung auf Deutsch:

Durch einen Hackerangriff Anfang 2023 wurde bekannt, dass die Medienaufsichtsbehörde Roskomnadsor zwischen 2020 und 2022 Datenlisten geführt hat, auf denen Tausende von LGBTQ-Aktivistinnen und -Aktivisten, NGOs, Medienschaffende und Redaktionen und Oppositionelle erfasst wurden. In den enthüllten Listen standen 1.246 Namen und 113 Bezeichnungen von Medien und Organisationen, darunter bekannte Telegram- und YouTube-Kanäle. Diese Daten dienten vermutlich als Grundlage für die Einstufung als „ausländischer Agent" sowie zur digitalen Überwachung russischer Staatsangehöriger, welche der Behörde verdächtig erschienen.

Eine vollumfängliche Überwachung russischer Staatsangehöriger durch Roskomnadsor ist derzeit technisch möglich. Anfang 2023 wurde bekannt, dass Roskomnadsor ein einheitliches System zur Überwachung in sozialen Netzwerken sowie im gesamten Internet aufbauen will. Zu diesem Zweck werden mehrere technische Überwachungssysteme verwendet. „Oculus" sucht seit Mitte Februar 2023 nach verbotenen (nach der russischen Gesetzgebung illegalen) Inhalten im Internet, nach offiziellen Angaben, nach „LGBTQ-Propaganda", „Aufrufen zu illegalen Aktivitäten", Aufrufen zum Selbstmord, Drogenverbreitung und extremistischen Inhalten. Insbesondere durchsucht „Oculus" Bilder und Videos. Ein weiteres Überwachungssystem, „Vepr", dient dem Zweck, Internet-Ressourcen mit einem täglichen Nutzerverkehr von mindestens einer Million Personen abzudecken, um „verbotene oder störende Inhalte" in Texten und Videos (darunter auch in Streaming-Videos) zu erkennen.

Diese selbstlernenden, auf neuronalen Netzwerken basierten Überwachungssysteme sollen es unter anderem ermöglichen, sogenannte Gefährderprofile festzustellen und zu überwachen und helfen bei der Zensur.

A huge amount of documents from Roskomnadzor was published[34] by journalists in early 2023. The Belarusian hacking collective „Cyber Partisans" took responsibility for the hack. This leak was called „Russian Censorship Documents" (RussianCensorFiles). It shows that in addition to preparing references to „foreign agents", the agency also illegally collected massive amounts of data and made references to people from 2020 to 2022. There were thousands of names on the lists, mostly employees of media outlets, NGOs, LGBT organizations, and activists. It can be assumed that these lists are further used to include citizens in the lists of foreign agents, as well as persons affiliated with foreign agents (such notion appeared in the Russian legislation after the new version of the „law on foreign agents" came into force on December 1, 2022), as well as for increased monitoring of citizens with perceived „deviant" behavior.

The lists revealed 1,246 unique names and 113 media and organizations. The information notes were prepared not only for organized media, but also for individual popular Telegram and Youtube

34 iStories, More than 100 new names appeared on the list of potential 23 foreign agents (https://istories.media/news/2023/02/23/v-spiske-potentsialnikh-inoagentov-poyavilos-bolee-100-novikh-imen).

channels and other media projects. As of today, more than 160 people and 17 media outlets from this list have already been recognized as foreign agents. The information notes[35] were compiled not only for Russian citizens. Ukrainian public figures, Belarusian journalists, and Georgian political scientists were also found on the lists.

Most of the people on the list are journalists, but there are also many activists from different spheres. In the documents there are also state deputies of different levels, a total of 13 people. The list of 114 organizations consists of 60% mass media, 10% human rights organizations, 5% election observation NGOs, and 4% LGBTQ organizations. Both authors of the report found their colleagues, including editors, system administrators, and attorneys, on that list of monitoring.

By indirect signs, we can assume that these information notes are further used to include citizens and organizations in the lists of foreign agents, undesirable and banned organizations as well as persons affiliated with foreign agents (such notion appeared in the Russian legislation after the new version of the „law on foreign agents" came into force on December 1, 2022). The information collected about individuals and organizations can be also used by the authorities to increase the monitoring of social media activity against people with deviant, politically disloyal behavior in order to prosecute them administratively and criminally.

In 2023, it was revealed that Roskomnadzor aimed to establish a unified surveillance system for social networks and the entire Russian internet. The agency is concurrently developing two AI systems intended to combat misinformation and illicit content. In mid-February 2023, **Roskomnadzor launched „Oculus," an automated system** to detect prohibited content in images and videos, including extremist material, calls for illegal activities, suicide, drug-related content, and LGBT propaganda. **Another system, „Vepr", is slated to monitor platforms with a daily audience of at least one million people** and identify banned or disturbing content in texts and videos, including streaming videos. While the organization, a subsidiary of Roskomnadzor, asserts that the primary aim of creating such a system is to automate the detection of violations of Russian laws in internet images and videos and optimize the associated costs, concerns are raised that the deployment of machine learning-based surveillance systems will enable authorities to automate censorship, prosecute users for posting illegal content, and profile „dangerous users" for additional surveillance.

35 Chronicles Media, https://chronicles.media/inoagenty-roskomnadzor.

GENERAL DATA SECURITY / ALLGEMEINE DATENSICHERHEIT

Zusammenfassung auf Deutsch:

Seit dem 24.02.2022 wurden personenbezogene Daten von insgesamt etwa 75 % aller russischen Staatsangehörigen (99.9 Millionen Email-Adressen und 109.7 Millionen Handynummern) im Internet geleakt. Dies geschah durch Hackerangriffe auf staatliche Dienste wie Sberbank, Russische Post, Agentur der Strategischen Initiativen und andere sowie auf kommerzielle, nichtstaatliche Internetdienste wie Yandex, die Logistikdienstleister SDEK, Delivery Club und andere. Der russische Staat scheint aufgrund bereits früher bestehender Probleme nicht in der Lage oder nicht willens zu sein, personenbezogene Daten russischer Staatsangehöriger zu schützen, ganz unabhängig von der politischen Einstellung dieser Personen.

Despite the facts that the Federal Law „On Personal Data" has been in force for over 13 years and the Russian Federation itself is a party to the Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, the situation with the protection of the right to privacy in the country is becoming alarming.

According to analysts36 2022 was a record year in terms of personal data leaks. During the year, 260 personal data leaks occurred, leaking a total of data of 75 % of Russian citizens, 99.8 million unique email addresses and 109.7 million unique telephone numbers. Leaks occurred both on the side of the largest private Internet companies (Yandex, SDEK, Delivery club), and on the side of state companies (Sberbank, Russian Post, the Agency for Strategic Initiatives). Most experts attributed37 the mass leaks to the start of the full-scale war with Ukraine since most of these leaks were due to hacker attacks. A distinctive feature of the last year was the fact that leaked and stolen databases are no longer sold on the darknet, but posted on free public access sites.38 The war revealed problems in legislation and law enforcement that had been ignored for years: extremely low penalties for companies, no requirements for information security, poor judicial practice with very little compensation for users if the data was leaked or the privacy rights were violated and the lack of an independent body to protect personal data of the people.

36 Data Leakage & Breach Intelligence, Overview of the black market of billing of Russian individuals for 2022, https://dlbi.ru/illegal-search-in-bases-review-2022.

37 Network Freedoms, The war of leaks (https://drive.google.com/file/d/1UA_D9DHcQ5iBNw3gkFsM_LKu5ub69yUk/view).

38 Roskomsvoboda: Report on Personal Data Leak from December 2022, https://roskomsvoboda.org/en/post/setevye-svobody-utechki.

Authors / Autoren:

Galina Arapova – Mass Media Defence Centre, head and senior media lawyer / Leiterin und leitende Medienanwältin des *Mass Media Defence Centers*.

Sarkis Darbinyan – lawyer at RosKomSvoboda, head and Managing Partner at Digital Rights Center / Rechtsanwalt bei RosKomSvoboda, Leiter und geschäftsführender Gesellschafter des *Digital Rights Centers*.

Inhaltliche Zusammenfassung auf Deutsch: Reporter ohne Grenzen e.V.