

# **О НОВЫХ СПОСОБАХ, НОРМАХ И ТЕХНОЛОГИЯХ СЛЕЖКИ ЗА ИНОСТРАННЫМИ ГРАЖДАНАМИ В РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Доклад аналитической службы  
Сети «Миграция и Право»**



**Автор: Константин Троицкий — руководитель  
аналитической службы Сети «Миграция и Право»**

## **Содержание**

Введение .....	3
Аббревиатуры некоторых основных систем и баз данных, используемых российскими властями.....	9
1. Подача на визу и заявление о въезде / сбор анкетных и биометрических данных..	10
2. На пограничном пункте / проверки и дальнейший сбор данных .....	13
3. Перемещение / система видеонаблюдения .....	14
4. Пользование телефоном и Интернетом / мониторинг и цензура.....	18
5. Общение/ распознавание речи .....	23
6. Пользование транспортом и услугами гостиничного комплекса / проверки и отслеживание передвижения .....	25
7. Постановка на учет / установка приложения по слежке .....	27
8. Оформление миграционных документов / геномная регистрация .....	28
9. Банковские операции, переводы, покупки и доставка / усиленное внимание.....	30
10. Попадание в реестр контролируемых лиц / ограничения и высылка из России...31	
Заключение .....	35
Использованная литература и нормативные акты .....	36

## Введение

Практики наблюдения (*surveillance*)<sup>1</sup> – неотъемлемая часть истории человечества<sup>2</sup>. Однако, если раньше наблюдение было сильно ограничено, то с внедрением новых технологий и переходом на цифровой формат, позволяющий передавать, накоплять, хранить и анализировать разнообразные данные, наблюдение вышло на иной уровень по охвату, глубине и комплексности. Это сделало необходимым, согласно некоторым исследователям, разделять между “традиционным наблюдением” (*traditional surveillance*), опирающимся на прямой визуальный/слуховой контакт и примитивные средства учета, от “нового наблюдения” (*new surveillance*), строящееся вокруг передовых цифровых технологий<sup>3</sup>.

Наблюдение – амбивалентный и многоаспектный феномен; с разными целями наблюдение ведут международные корпорации и частные лица, банки и операторы связи, СМИ и адвокаты, медицинские учреждения и спортивные клубы, аэропорты и гостиницы, образовательные учреждения и благотворительные фонды, исследовательские центры и заводы, преступники и следователи, транспортные службы и строители, муниципалитеты и государственные ведомства, интернет-платформы и мессенджеры… и так далее. В развитом обществе при участии новых технологий а) все являются объектами наблюдения (государственный учет, трекеры в Интернете, видеокамеры, спутники, системы идентификации и регистрации, медицинские анализы и так далее), б) многие наблюдают друг за другом (мобильные приложения, фото и видеофиксация, дроны, социальные сети и так далее) и в) некоторые занимаются самонаблюдением (мобильные приложения, электронные дневники, “умные часы” и так далее)<sup>4</sup>.

Поэтому при принятии перспективы прав человека основные вопросы касаются не того допускать или не допускать наблюдение, а на каких принципах оно основывается, то есть во имя чего проводится, как именно ведется, существует ли независимый общественный контроль за его реализацией. Это особенно касается наблюдения со стороны государства, что стало постоянной темой многих подразделений ООН<sup>5</sup>, а правозащитные и экспертные организации сформулировали принципы, которым государства должны следовать при внедрении и использовании технологий по наблюдению<sup>6</sup>. Так, одно дело, если

---

<sup>1</sup> В англоязычной и франкоязычной литературе для обозначения особого и систематического внимания к личным данным, передвижению, поведению и привычкам людей используется термин “*surveillance*”, для которого в русском языке нет однозначного эквивалента. В зависимости от контекста, этот термин переводится на русский язык словами “слежка”, “наблюдение”, “отслеживание”, “надзор”, “мониторинг”, “опека”, “контроль”. В рамках нашего доклада речь мы будем преимущественно использовать а) слово “наблюдение”, когда речь идет о *surveillance* в общем, а также в правовых демократических государствах и б) слово “слежка”, когда речь идет о *surveillance* в полицейских и разведывательных целях, а также в авторитарных государствах.

<sup>2</sup> Weller, Toni. “The historical ubiquity of surveillance”. In edited by Andreas Marklund & Laura Skouwig, *Histories of Surveillance from Antiquity to the Digital Era*. London and New York, Routledge, 2022. P. 175.

<sup>3</sup> Marx, Gary. *Windows into the Soul. Surveillance and Society in an Age of High Technology*. The University of Chicago Press, 2016. P. 15-18.

<sup>4</sup> Краткое введение в феномен “наблюдения”, его многообразие, сложность и амбивалентность дано, например, здесь: Lyon, David. *Surveillance*. Oxford, Oxford University Press, 2024.

<sup>5</sup> О взгляде ООН на соотношение наблюдения (слежения) и прав человека см., например: Доклад Специального докладчика ООН по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. “Слежение и права человека”. *Совет по правам человека*. Сорок первая сессия 24 июня – 12 июля 2019 года. <https://digitallibrary.un.org/record/3814512?ln=en&v=pdf> (Доступ: 17.08.2025), а также Доклад Управления Верховного комиссара Организации Объединенных Наций по правам человека. “Право на неприкосновенность частной жизни в цифровую эпоху”. *Совет по правам человека*. Пятьдесят первая сессия 12 сентября – 7 октября 2022 года <https://docs.un.org/ru/A/HRC/51/17> (Доступ: 08.08.2025).

<sup>6</sup> См., например, 13 принципов, разработанные экспертами в области новых технологий и правозащитниками, здесь: Access, EFF, Privacy International, et. al. “Международные принципы по соблюдению прав человека при

государственное наблюдение имеет цель защищать основные права и свободы человека, ведется с соблюдением четких норм, контролируется независимыми правозащитными и экспертными организациями. Совершенно другое дело, если наблюдение используется для укрепления и удержания власти, не регламентируется четкими правовыми нормами, а какой-либо независимый правозащитный контроль за ее проведением попросту отсутствует. В последнем случае речь идет об авторитарных режимах. Если такие режимы в удержании и укреплении своей власти во многом опираются на цифровые технологии, то исследователи обозначают их суть как цифровой авторитариализм<sup>7</sup>, а в случае активного вовлечения новейших технологий, включая технологии на базе искусственного интеллекта, как алгоритмический авторитаризм<sup>8</sup>.

В авторитарных режимах системы наблюдения во многом обращаются в то, что следует называть системой слежки, поскольку приобретают всеохватывающий характер и становятся элементом репрессивной системы. Слежка ведется с целями контроля всех более или менее существенных социальных, культурных, экономических и политических процессов, служит повышению эффективности массовой пропаганды и дезинформации, а также непосредственно или опосредованно используется для репрессий в отношении оппозиции<sup>9</sup>. Дополнительную эффективность этим системам слежки придает развитие новых технологий и тесное взаимодействие авторитарных режимов между собой, что позволяет им среди прочего обмениваться технологиями, данными и практиками, обходить санкции, выстраивать общие кампании по дезинформации и координировать репрессивные действия<sup>10</sup>. Все более активное использование авторитарными режимами технологий искусственного интеллекта для слежки и репрессий вызывает у экспертов и правозащитников особую озабоченность<sup>11</sup>.

Мы будем исходить из следующего определения: государственное наблюдение – любое рутинное, массовое, сфокусированное и систематическое внимание государственных органов и аффилированных с ними агентов к личным данным и поведению в целях управления, защиты, контроля, а также, в случае авторитарных режимов, для репрессий в отношении политических оппонентов, правозащитников, журналистов, независимых организаций и общественных активистов<sup>12</sup>.

История наблюдения/слежки в российской истории уходит в глубину веков, но систематический и масштабный характер приобретает вместе со становлением сильного

---

использовании слежки в коммуникациях”  
<https://necessaryandproportionate.org/ru/%D0%BF%D1%80%D0%B8%D0%BD%D1%86%D0%B8%D0%BF%D1%8B/> (Доступ: 19.08.2025).

<sup>7</sup> Подробно об определении и аспектах цифрового авторитариализма см., например: Pearson, James. S. “Defining Digital Authoritarianism”. *Philosophy & Technology*. 2024. Vol. 37. No. 73. <https://link.springer.com/article/10.1007/s13347-024-00754-8#Fn2> (accessed October 4, 2025)

<sup>8</sup> См., например: Ünver, A. *Artificial intelligence (AI) and human rights: Using AI as a weapon of repression and its impact on human rights*. Brussels, European Union, 2024 [https://www.europarl.europa.eu/thinktank/en/document/EXPO\\_IDA\(2024\)754450](https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2024)754450) (accessed August 19, 2025).

<sup>9</sup> См., например: Feldstein, Steven. *The Rise of Digital Repression. How Technology Is Reshaping Power, Politics, and Resistance*. Oxford, Oxford University Press, 2021; Pei, M. *The Sentinel State. Surveillance and the Survival of Dictatorship in China*. Cambridge, Harvard University Press, 2024; Gohdes, A.R. *Repression in the Digital Age. Surveillance, Censorship, and the Dynamics of State Violence*. Oxford, Oxford University Press, 2024.

<sup>10</sup> См., например, Applebaum, A. *Autocracy, INC. The Dictators Who Want to Run the World*. New York, Doubleday, 2024.

<sup>11</sup> См., например: Ünver, A. *Artificial intelligence (AI) and human rights: Using AI as a weapon of repression and its impact on human rights*. Brussels, European Union, 2024 [https://www.europarl.europa.eu/thinktank/en/document/EXPO\\_IDA\(2024\)754450](https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2024)754450) (accessed August 19, 2025).

<sup>12</sup> Определение наблюдения/слежки составлено, хотя не сводится, к определению, которое предложено в Lyon, David. *Surveillance*. Oxford, Oxford University Press. 2024.

централизованного государства. К концу XIX века и начало XX века в Российской империи установилась сеть наблюдения/слежки, состоящая из систем все более усложняющегося учета, а также информаторов, провокаторов и доносчиков<sup>13</sup>. Однако, все это затмила советская система слежки, ставшая элементом репрессивных практик, которые в сталинский период достигли небывалых за всю историю человечества размеров, изощренности и жестокости<sup>14</sup>. В конце 1980-х и начале 1990-х годов слежка в СССР, а затем в Российской Федерации находилась в периоде “перестройки”, что дало надежду на возможность образования современной государственной системы наблюдения, которая бы базировалась на уважении к правам человека и находилась бы под общественным контролем. Этим надеждам не суждено было сбыться. Уже с самого начала 2000-х годов российские власти принялись выстраивать новое авторитарное государство, в центре которого расположились неподотчетные обществу спецслужбы, одержимые слежкой и контролем<sup>15</sup>.

Рост авторитарных тенденций начала 2000-х годов в России совпал с появлением невиданных дотоле технологий наблюдения<sup>16</sup>. Задействуя цифровые технологии, российские власти начали активно выстраивать новую систему слежки, состоящую из замысловатых и многочисленных баз данных, сетей видеокамер, комплекса по прослушке телефонов, мониторинга Интернета, надзора за банками, аналитических центров, научно-исследовательских предприятий, что опиралось на выпуск новых репрессивных нормативных актов<sup>17</sup>. С конца 2010-х годов власти стали активно и систематически применять новую систему слежки не только для фиксации преступлений и поиска подозреваемых, но также для преследования политической оппозиции, неугодных журналистов, правозащитников и гражданских активистов. Российские власти давно игнорируют рекомендации ООН по использованию технологий<sup>18</sup>, а выстроенная система слежки не отвечает международным правовым требованиям и используется для репрессивных целей, что неоднократно

---

<sup>13</sup> См., например: Zuckerman, Fredric S. *The Tsarist Secret Police in Russian Society, 1880-1917*. New York, New York University Press, 1996.

<sup>14</sup> О связи слежки и репрессии в СССР сталинского периода см., например: Shearer, David R. *Stalin's Socialism. Repression and Social Order in the Soviet Union, 1924-1953*. New Haven and London, Yale University Press, 2009 (в переводе на русский язык “surveillance” переводится как “надзор”, см.: Ширер, Дэвид. Р. *Сталинский военный социализм. Репрессии и общественный порядок в Советском Союзе, 1924-1953 гг.* Москва, РОССПЭН, 2014).

<sup>15</sup> См., например: Солдатов Андрей и Ирина Бороган. *Новое дворянство: Очерки истории ФСБ*. Москва, Альпина Бизнес Букс, 2012.

<sup>16</sup> О новых технологиях наблюдения, появившихся на стыке XX и XXI веков см. например: Petersen, J.K. *Introduction to Surveillance Studies*. Boca Raton, Taylor & Francis Group, 2013.

<sup>17</sup> См., например: Mahon, Anastassiya and Scott, Walker. “Russia’s Digital Repression Landscape: Unraveling the Kremlin’s Digital Repression Tactics.” *Journal of Illiberalism Studies* 4 no. 3 (Fall 2024): 29-50; International Partnership for Human Rights (IPHR) and Global Diligence LLP. “Russia’s Digital Authoritarianism: the Kremlin’s Toolkit,” September, 2023 <https://iphronline.org/articles/russias-digital-authoritarianism-the-kremlins-toolkit/> (accessed August 12, 2025).

<sup>18</sup> См.: Доклад Управления Верховного комиссара ООН по правам человека. “Права человека и новые и появляющиеся цифровые технологии”. *Совет по правам человека*. Пятьдесят шестая сессия 18 июня — 12 июля 2024 года. <https://docs.un.org/ru/A/HRC/56/45> (Доступ: 08.08.2025) и Доклад Управления Верховного комиссара Организации Объединенных Наций по правам человека. “Право на неприкосновенность частной жизни в цифровую эпоху”. *Совет по правам человека*. Пятьдесят первая сессия 12 сентября — 7 октября 2022 года <https://docs.un.org/ru/A/HRC/51/17> (Доступ: 08.08.2025).

фиксировалось журналистами<sup>19</sup>, правозащитниками<sup>20</sup>, Комитетом по правам человека ООН<sup>21</sup> и Европейским судом по правам человека (Zakharov v. Russia, Glukhin v. Russia, Podchasov v. Russia).

Иностранные граждане<sup>22</sup> в России давно испытывают на себе особое внимание российских силовых ведомств. Трудовые мигранты из Центральной Азии, беженцы и лица, ищущие убежище находятся в России в особо уязвимом положении, становясь жертвами ксенофобии, систематической дискриминации, бюрократического и полицейского произвола, что усугубилось с начала антимигрантской кампании в марте 2024 года<sup>23</sup>. В последние годы российские власти обычно уже даже формально не декларируют необходимость защиты прав мигрантов. Так, например, в “Концепции государственной миграционной политики Российской Федерации на 2019-2025 годы” говорится о демографии, экономике, безопасности и контроле, но отсутствует даже упоминание о необходимости защиты прав человека, а трудовая миграция представляется как вынужденная мера, чреватая опасностями и нуждающаяся в строжайшем наблюдении и контроле<sup>24</sup>. Как итог, российские власти ищут и изобретают способы для более активного применения новых технологий для слежки за мигрантами.

Процесс развития системы тотальной слежки на территориях, контролируемых российскими властями<sup>25</sup>, ускорился в 2020-х годах, а 2024 и 2025 годы стали поворотным моментом,

<sup>19</sup> См., например: Легалов, Евгений. “Небольшой брат. Как видеокамеры стали инструментом репрессий”. *Radio Svoboda* (07.05.2024) <https://www.svoboda.org/a/neboljshoy-brat-kak-videoekamery-stali-instrumentom-repressiy/32932369.html> (Доступ: 15.08.2025); Reporters Without Borders. “Taking Control? Internet Censorship and Surveillance in Russia.” 2019. [https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Downloads/Berichte/2019/russiareport\\_web\\_updated.pdf](https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Downloads/Berichte/2019/russiareport_web_updated.pdf) (accessed August 18, 2025); Krolik, A.; Mozur, P.; Satariano, A. “Cracking Down on Dissent, Russia Seeds a Surveillance Supply Chain”. *The New York Times* (03.07.2023) <https://www.nytimes.com/2023/07/03/technology/russia-ukraine-surveillance-tech.html> (accessed August 19, 2025).

<sup>20</sup> См., например: ОВД-Инфо. “Как власти используют камеры и распознавание лиц против протестующих.” 17.02.2022, <https://reports.ovd.info/kak-vlasti-ispolzuyut-kamery-i-raspoznavanie-lic-protiv-protestuyushchih> (доступ 12 августа 2025 года); ОВД-Инфо и Роскосвобода. “Права человека и новые технологии в России.” 06.03.2023, <https://reports.ovd.info/prava-cheloveka-i-novye-tehnologii-v-rossii> (доступ 8 августа 2025 года); International Partnership for Human Rights (IPHR) and Global Diligence LLP. “Russia's Digital Authoritarianism: the Kremlin's Toolkit.” September, 2023 <https://iphronline.org/articles/russias-digital-authoritarianism-the-kremlins-toolkit/> (accessed August 12, 2025); Human Rights Watch. “Disrupted, Throttled, and Blocked State Censorship, Control, and Increasing Isolation of Internet Users in Russia”. July, 2025 [https://www.hrw.org/sites/default/files/media\\_2025/07/russia0725%20web.pdf](https://www.hrw.org/sites/default/files/media_2025/07/russia0725%20web.pdf) (accessed August 8, 2025).

<sup>21</sup> См., например: Комитет по правам человека ООН. “Заключительные замечания по восьмому периодическому докладу Российской Федерации” (октябрь-ноябрь 2022) <https://docs.un.org/ru/CCPR/C/RUS/CO/8> (Доступ: 15.08.2025).

<sup>22</sup> Здесь и далее термины “иностранные граждане” и “мигранты” используются как синонимы и подразумевают все категории иностранных граждан, включая туристов.

<sup>23</sup> См., например: Human Rights Watch. “Living in Fear and Humiliation. Rising Xenophobic Harassment and Violence towards Central Asian Migrants in Russia”. March, 2025 [https://www.hrw.org/sites/default/files/media\\_2025/04/russia0325web.pdf](https://www.hrw.org/sites/default/files/media_2025/04/russia0325web.pdf) (accessed August 22, 2025)

<sup>24</sup> См.: Указ Президента РФ от 31.10.2018 N 622 “О Концепции государственной миграционной политики Российской Федерации на 2019 - 2025 годы” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_310139/74e338ae02b148ec31de4bc38f486b8b045d3a1e/](https://www.consultant.ru/document/cons_doc_LAW_310139/74e338ae02b148ec31de4bc38f486b8b045d3a1e/) (Доступ: 15.08.2025).

<sup>25</sup> С 2014 года Крым, а с четвертого квартала 2022 года Запорожскую, Херсонскую, Донбасскую и Луганские области Украины, российские власти стали рассматривать как части Российской Федерации. Генеральная Ассамблея ООН несколько раз подавляющим большинством голосов осудила агрессивные действия российского государства в отношении Украины и не считает указанные выше территории частями Российской Федерации. Однако, российские власти цинично проигнорировали резолюции высшей инстанции международного сообщества. Чтобы не оговаривать этот каждый раз, следует сразу пояснить, что ниже выражения “Россия” или “Российская Федерация”, особенно когда речь идет о событиях после марта 2014 года, используются не в смысле

поскольку помимо расширения и усиления уже действующих способов слежки (например, сбор и анализ анкетных данных, биометрия фотографий, регистрация СИМ карты на конкретного пользователя, системы видеонаблюдения, мониторинг в Интернете, прослушка телефонов) в течение короткого времени для всех или в некоторых случаях для основных категорий мигрантов были введены сразу несколько новых (голосовая биометрия, сбор данных о геолокации и установка приложения по слежке за пользователем, геномная регистрация, обязательное закрепление мобильного телефона и СИМ карты за конкретным человеком).

Новейшие тенденции нашли отражение в “Концепции государственной миграционной политики Российской Федерации на 2026-2030 годы”. В этом документе по-прежнему отсутствует даже упоминание необходимости защиты прав человека, а по сравнению с версией на 2019-2025 годы еще больший акцент поставлен на развитии, внедрении и применении цифровых технологий для “контроля” (читай слежки) за мигрантами, включая перечисление некоторых таких технологий. Так, в тексте этой концепции среди общих формулировок конкретно оговаривается стремление властей по дальнейшему развитию и расширению: 1) “профилирования данных об иностранных гражданах”, 2) сбора биометрических данных за границей, 3) практики уведомлений “о планируемом въезде”, а также 4) технологий на базе искусственного интеллекта для “обработки большого массива данных”<sup>26</sup>.

В нашем докладе мы дадим краткое описание систем слежки за мигрантами. Мы делаем акцент на том, как система функционирует для иностранного гражданина, который решил поехать в Россию, не углубляясь в детали, как сложная российская система слежки устроена. Изучение деталей не только бы потребовало во много раз более объемного исследования, но и неминуемо привело бы к включению домыслов и догадок, поскольку российскую систему отличает секретность, неподотчетность и сложность. Так, например, в подчинении мэрии Москвы, известной своим стремлением к тотальной слежке, только официально действует около двух сотен разнообразных информационных систем, а МВД России образуют сложную и запутанную структуру, включающую десятки крупных модулей и систем, о подробностях функционирования которых из открытых источников известно крайне мало.

Как итог, в обзоре мы рассказываем лишь о некоторых известных и важнейших (по нашему мнению) технологиях, способах и стратегиях, которые используют российские власти при слежке за иностранными гражданами. Мы также делаем акцент на описании ряда нормативных нововведений последних двух лет, которые расширяют и без того аномально широкие полномочия государственных ведомств. Важно также иметь в виду, что хотя некоторые новые способы слежки направлены исключительно на иностранных граждан, большинство технологий используется российскими властями для слежки и за гражданами России.

Для целей нашего доклада среди многочисленных стратегий наблюдений следует выделить две огромные группы. Первая из них направлена преимущественно на общее наблюдение, то есть направлена либо на всех, кто попадает в досягаемость систем наблюдения, либо на большие категории граждан (например, дети, мужчины, женщины, чернокожие, дворники, мигранты). Вторая группа, которую можно назвать “целевым наблюдением” (targeted

---

российской территории в признанных и правовых границах, а являются синонимом территорий, контролируемых российскими властями.

<sup>26</sup> Указ Президента РФ от 15..10.2025 N 738 “О Концепции государственной миграционной политики Российской Федерации на 2026 - 2030 годы” <https://www.garant.ru/hotlaw/federal/1887540/> (Доступ: 17.10.2025).

surveillance)<sup>27</sup> относится к отслеживанию личных данных и действий конкретного человека или небольших групп людей. Многие технологии и способы, которые используются для общего наблюдения (системы видеонаблюдения, мониторинг интернета, миграционный учет, отслеживание финансовых операций и так далее), применяются и для целевого наблюдения. Однако, последняя стратегия знает и свои специфические приемы и технологии, например, “наружное наблюдение”, взлом аккаунтов и мобильных устройств, использование “жучков” и скрытых видеокамер, незаметная установка программ по слежке и так далее. В нашем докладе речь пойдет в основном об общем наблюдении с акцентом на слежке за мигрантами на территории, контролируемой российскими властями. Мы не пишем о слежке вне таких территорий, также не рассматриваем тему целевой слежке за отдельными иностранными гражданами, которые ведут российские власти в рамках шпионской, контрразведывательной, либо оперативно-розыскной деятельности. Это отдельные темы, которые покрыты особо плотным занавесом секретности.

И последнее вводное замечание: в целях удобства изложения мы представим материал поэтапно, то есть начинаем с описания того, как российские власти собирают данные при подаче иностранным гражданином заявления на российскую визу или просьбы о разрешении на въезд, продолжаем рассказом о том, какие технологии и способы слежки активируются в момент въезда иностранного гражданина в Россию и заканчиваем повествование моментом добровольного выезда или принудительного выдворения мигранта<sup>28</sup>.

---

<sup>27</sup> В разделении на общее и целевое наблюдение мы основываемся на классификацию стратегий наблюдений, которую предложил Стивен Фельдштейн. Впрочем, следует отметить, что Фельдштейн выделил четыре стратегии: пассивное наблюдение (passive surveillance), целевое наблюдение (targeted surveillance), наблюдение на основе ИИ и анализа больших данных (AI and big-data surveillance), законы и директивы (surveillance laws and directives), см.: Feldstein, Steven. *The Rise of Digital Repression. How Technology Is Reshaping Power, Politics, and Resistance*. Oxford, Oxford University Press, 2021. P. 27-30.

<sup>28</sup> В случаях так называемого целевой слежки она может продолжаться и после выезда из России.

## **Аббревиатуры некоторых основных систем и баз данных, используемых российскими властями**

**АИС Консул-ЗУ** - Автоматизированная информационная система “Консул-ЗУ” (в загранучреждениях)

**АИС Криминал-И** - Автоматизированная информационная система “Криминал-И”

**АС ОПИГ** - Автоматизированная система оформления приглашений иностранным гражданам

**АС ЦБД УИГ** - Автоматизированная Система Центрального Банка Данных по Учету Иностранных Граждан и лиц без гражданства

**АЦБПДП** - Автоматизированные централизованные базы персональных данных о пассажирах и персонале (экипаже) транспортных средств

**ГАИС Сфера** - Государственная автоматизированная информационная система “Сфера”

**ГС МИР** - Государственная система миграционного и регистрационного учета, а также изготовления, оформления и контроля обращения документов, удостоверяющих личность

**ЕБС** - Единая биометрическая система

**ЕГИС ОТБ** - Единая государственная информационная система обеспечения транспортной безопасности

**ЕПГУ** - Единый портал государственных и муниципальных услуг

**ЕСИА** - Единая система идентификации и аутентификации

**ЕСМЭВ** - Единая система межведомственного электронного взаимодействия

**ЕЦХД** - Единый центр хранения данных (Москва)

**Реестр ОРИ** - Реестр организаторов распространения информации

**РКЛ** - Реестр контролируемых лиц

**СОРМ** - Система оперативно-розыскных мероприятий

**ФБД ГeН** - Федеральная база данных геномной информации

**ЦФ ИГ** - Цифровой профиль иностранного гражданина

**MOS ID** - Система аутентификации и регистрации для доступа к цифровым ресурсам города Москвы

**ruID** - Мобильное приложение единого портала

## **1. Подача на визу и заявление о въезде / сбор анкетных и биометрических данных**

Требования к оформлению документов для въезда зависят от того, гражданином какой страны является человек, желающий приехать в Российскую Федерацию. Если у человека паспорт страны, для граждан которой предусмотрен визовый порядок, то он оформляет визу, если страны, для которой предусмотрен безвизовый порядок, то с 2025 года российские власти рекомендуют ему подать заявление о въезде, которое пока носит добровольный характер, но с высокой долей вероятности можно предположить, что у российских властей существуют планы сделать подачу такого заявления обязательным.

### **Визы**

Визовые требования отличаются в зависимости от целей поездки, а также от того, входит ли страна, гражданин которой изъявляет желание посетить Россию, в список стран, для граждан которых возможно оформление так называемых “электронных виз” или нет. Если речь идет об оформлении визы в обычном порядке, то МИД России организовал заполнение анкеты на визы через их официальный сайт. Таким образом, еще даже до подачи иностранным гражданином документов в визовый отдел российские власти видят, кто думает о поездке в Россию. Далее, консульские сотрудники требуют, чтобы анкета была распечатана, подписана, подкреплена фотографией и документами, которые варьируются в зависимости от заявителя и целей поездки. В самой анкете обычно требуется указать персональные данные (ФИО, дата и место рождения, гражданский статус, наличие детей и т.п.), контактную информацию (телефон, адрес электронной почты, адрес проживания и т.п.), а также иные сведения (место работы, информация о посещении России в прошлом, цели поездки, место проживания в России, наличие родственников в России и т.п.).

Все эти данные попадают в базы данных МИД РФ (“Автоматизированную систему оформления приглашений иностранным гражданам” (АС ОПИГ) или в Автоматизированную информационную систему Консул-ЗУ (АИС Консул-ЗУ)<sup>29</sup> и направляются в ФСБ России, которое уведомляет о том, может ли данный гражданин въехать в Россию или нет. Сведения также загружаются в “Государственную систему миграционного и регистрационного учета” (далее – ГС МИР), доступ к которой имеют ряд других российских ведомств<sup>30</sup>. Согласно Постановлению Правительства РФ от 7 ноября 2024 года, фотография и сведения, полученные при оформлении визы, поступают в “Единую систему идентификации и аутентификации” (далее – ЕСИА), а также в связанную с ней “Единую биометрическую систему” (далее – ЕБС)<sup>31</sup>. На ЕСИА и ЕБС в частности строится работа “Единого портала государственных и муниципальных услуг (функций)” (далее – ЕПГУ).

С 2023 года органы МИД России стали выдавать гражданам некоторых стран так называемые “электронные визы”. Порядок оформления этого типа виз не требует личного посещения

---

<sup>29</sup> Приказ МИД России от 31.05.2017 N 9175 “Об утверждении Порядка организации деятельности Министерства иностранных дел Российской Федерации по оформлению, выдаче, продлению срока действия визы, восстановлению либо аннулированию визы, а также порядка учета и хранения бланков виз” <https://base.garant.ru/71709404/> (Доступ: 17.08.2025).

<sup>30</sup> См. пункт 15 здесь: Постановление Правительства РФ от 06.08.2015 N 813 (ред. от 21.10.2024) “Об утверждении Положения о государственной системе миграционного и регистрационного учета, а также изготовления, оформления и контроля обращения документов, удостоверяющих личность” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_184040/](https://www.consultant.ru/document/cons_doc_LAW_184040/) (Доступ: 17.08.2025).

<sup>31</sup> См. пункт 10 здесь: Постановление Правительства Российской Федерации от 07.11.2024 N 1510 “О проведении эксперимента по апробации правил и условий въезда в Российскую Федерацию и выезда из Российской Федерации иностранных граждан и лиц без гражданства” <https://www.garant.ru/products/ipo/prime/doc/410628090/> (Доступ: 17.08.2025).

консульства и/или визового центра, а также обычно происходит за несколько дней. В то же время в отличии от обычных “электронные визы” предназначены исключительно для одного въезда и выезда и действительны лишь для поездок не более 30 дней. Российские власти оставляют за собой возможность в любой момент, включая прохождение пограничного контроля, аннулировать “электронную визу” без каких-либо объяснений<sup>32</sup>.

Кроме того, обращает на себя объем сведений, которые требуется от иностранного гражданина, желающего получить “электронную визу”. Так, помимо стандартных данных (ФИО, пол, семейное положение, дата рождения, цель поездки, рассчитываемый период пребывания, адрес предполагаемого проживания) требуется детально указать:

- список всех стран, в которых бывал посетитель за последние три года;
- персональные данные родителей, детей и супруга/и, а также их контактные данные, если они проживают в России;
- наличие недвижимости в России;
- список всех образовательных организаций, в которых обучался заявитель (не считая школ);
- если есть то место работы, если это не первое место работы, то два последних места работы;
- список мессенджеров и социальных сетей, которыми пользуется заявитель;
- наличие знаний и образования, связанных с “оружием, взрывчатыми, ядерными, биологическими или химическими веществами”;
- уровень военной подготовки и участие, если имело место, в военных конфликтах;
- связь или отсутствие оной с международными, некоммерческими и государственными организациями<sup>33</sup>.

Все эти данные и фотография загружаются в систему ГС МИР и иные базы данных, где к ним сразу получают доступ МВД и ФСБ, принимающие решение о пропуске или отказе в пропуске иностранного гражданина<sup>34</sup>.

### Заявления о въезде

До 2025 года перед иностранным гражданином, пользующимся безвизовым порядком въезда, не ставился вопрос о подготовке особых документов для въезда. С 2025 года в России действует “эксперимент” в ходе которого иностранному гражданину, прибывающему по безвизовому порядку, пока добровольно предлагается подать заявление о въезде (за исключением детей до шести лет, сотрудников дипломатических представительств и их семей, особых гостей и граждан Беларуси). Для подачи заявления о въезде требуется:

---

<sup>32</sup> См. пункты 13 и 14 здесь: Постановление Правительства РФ от 07.11.2020 N 1793 “О порядке оформления единых электронных виз и признании утратившими силу некоторых актов Правительства Российской Федерации” (вместе с “Положением о порядке оформления единых электронных виз”). [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_367444/47e1f3ca06b495c2673ba8e2e466a0fea84c4f8/](https://www.consultant.ru/document/cons_doc_LAW_367444/47e1f3ca06b495c2673ba8e2e466a0fea84c4f8/) (Доступ: 17.08.2025).

<sup>33</sup> Приказ МИД России от 14.12.2020 N 22683 “Об утверждении состава сведений, которые указываются иностранным гражданином в заявлении об оформлении единой электронной визы, а также форм уведомлений об оформлении и об отказе в оформлении единой электронной визы.” <https://base.garant.ru/400103460/> (Доступ: 21.08.2025).

<sup>34</sup> См. пункт 15-18 здесь: Постановление Правительства РФ от 06.08.2015 N 813 (ред. от 21.10.2024) “Об утверждении Положения о государственной системе миграционного и регистрационного учета, а также изготовления, оформления и контроля обращения документов, удостоверяющих личность” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_184040/](https://www.consultant.ru/document/cons_doc_LAW_184040/) (Доступ: 17.08.2025).

- Пройти процедуру “идентификации” и “аутентификации” на ЕПГУ (портал “Госуслуг”);
- Представить биометрические данные;
- Заполнить заявление о въезде с указанием ряда данных<sup>35</sup>.

Перечень сведений в заявлении устанавливается и проверяется рядом ведомств (МИД России, ФСБ, МВД, Минцифры), по результатам проверки иностранный гражданин может быть направлена информация об отказе во въезде. Для прохождения перечисленных выше процедур российские власти к 30 июня 2025 года создали мобильное приложение единого портала ruID (далее – ruID). Помимо биометрических данных (фотография, отпечатки пальцев, образец голоса) иностранного гражданина, желающего посетить Россию в безвизовом порядке, в приложении предлагается указать персональные данные (ФИО, дата рождения, гражданство), паспортные данные, цели въезда и срок пребывания в России, адрес проживания, контактную информацию. В случае разрешения на въезд иностранный гражданин получает QR-код, который он должен будет предъявить для сканирования на пограничном пункте.

На основании сведений, поданных через это приложение, еще до пересечения российских пограничных пунктов на иностранного гражданина составляется “цифровой профиль”, то есть своего рода “личное дело”, которое привязывается к нескольким информационным системам, включая ЕПГУ (Портал “Госуслуг”). Российские власти не устанавливают четких ограничений ни по перечню ведомств, имеющих доступ к цифровому профилю, ни по целям их использования, ни по сведениям, которые туда могут загружаться. Примечательно, что указ о создании информационной системы “Цифровой профиль иностранного гражданина” (далее – ЦФ ИГ)<sup>36</sup> появился в середине 2025 года, то есть значительно позже объявления о фактическом создании этого “цифрового профиля” в постановлении Правительства РФ от ноября 2024 года. На текущий момент известно, что в ЦФ ИГ загружаются личные данные, биометрические данные, контактные данные, сведения о документах (паспорт, миграционная карта, разрешение на работу и т.п.), история пересечений пограничных пунктов, место проживания и наличие постановки на учет, прохождение медицинского осмотра, налоговые сведения, информация о трудовой деятельности и социальных выплатах.

Судя по всему, российские власти планировали сделать подачу заявления обязательной уже с 30 июня 2025 года. Даже в самих “правилах эксперимента” говорится об “обязательности эксперимента”<sup>37</sup>. Однако, за две недели до обозначенной даты Минцифры, будучи помимо прочего разработчиком ruID, выпустило письмо о том, что отсутствие заявления о въезде пока не ведет к отказу во въезде<sup>38</sup>. Из новостей о ruID, из того факта, что это приложение появилось в последний момент, из того, что с разъяснением выступило Минцифры, к которому не относятся вопросы пересечения пограничных пунктов, следует предположить, что российские власти отменили обязательность заявления из-за серьезных технических недоработок системы

<sup>35</sup> См. пункт 5 здесь: Постановление Правительства Российской Федерации от 07.11.2024 N 1510 “О проведении эксперимента по апробации правил и условий въезда в Российскую Федерацию и выезда из Российской Федерации иностранных граждан и лиц без гражданства” <https://www.garant.ru/products/ipo/prime/doc/410628090/> (Доступ: 17.08.2025).

<sup>36</sup> См.: Указ Президента Российской Федерации от 09.07.2025 N 467 “О государственном информационном ресурсе ‘Цифровой профиль иностранного гражданина’” <https://www.garant.ru/products/ipo/prime/doc/412204934/> (Доступ: 18.08.2025).

<sup>37</sup> См. пункт 2 “Правил организации эксперимента” здесь: Постановление Правительства Российской Федерации от 07.11.2024 N 1510 “О проведении эксперимента по апробации правил и условий въезда в Российскую Федерацию и выезда из Российской Федерации иностранных граждан и лиц без гражданства” <https://www.garant.ru/products/ipo/prime/doc/410628090/> (Доступ: 17.08.2025).

<sup>38</sup> Письмо Минцифры России от 17.06.2025 N ОК-П24-58177 “О разъяснении правил, вводимых на территории Российской Федерации постановлением Правительства РФ от 07.11.2024 N 1510” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_509343/](https://www.consultant.ru/document/cons_doc_LAW_509343/) (Доступ: 18.08.2025).

и неготовности приложения ruID, а, возможно, и других информационных модулей. Ясно, что ситуация может быстро измениться и нет никаких оснований полагать, что у российских властей изменились планы и они отказались от идеи сделать подачу заявления и регистрацию в приложении ruID обязательной.

Ясно, что собранные через ruID данные и “цифровой профиль” облегчают российским властям слежку за иностранными гражданами.

## 2. На пограничном пункте / проверки и дальнейший сбор данных

Сотрудники ФСБ осуществляют пограничный контроль, к которому в частности относится проверка удостоверений личности на подлинность и наличие или отсутствие оснований для отказа во въезде. Вне зависимости от того предоставлял ли иностранный гражданин до этого свои биометрические данные (при получении визы, либо самостоятельно через ruID), сотрудники ФСБ вновь собирают и сверяют эти данные. Отказ от нового сбора биометрических данных ведет к запрету на въезд<sup>39</sup>. Примечательно, что на “период проведения эксперимента” это относится как к иностранным гражданам, которые пересекают пограничные пункты на въезд, так и к тем, кто выезжает<sup>40</sup>. Кроме того, при пересечении на въезд иностранный гражданин заполняет миграционную карту, сведения из которой сверяются с теми, которые иностранный гражданин указал при оформлении визы или заявлении на въезд.

Результаты всех этих проверок, а также факт пересечений пограничного пункта немедлено заносятся в базу ГС МИР<sup>41</sup>, в ЕСИА<sup>42</sup>, а также в иные базы данных. Многие из этих баз данных связаны между собой и в зависимости от полномочий и специфики деятельности к ним имеют доступы те или иные сотрудники государственных ведомств. Кроме того, российские власти разработали Единую систему межведомственного электронного взаимодействия (далее – ЕСМЭВ), которая позволяет разным государственным ведомствам, а также коммерческим организациям (прежде всего банкам и финансовым компаниям) обмениваться информацией друг с другом<sup>43</sup>.

ГС МИР также пополняется данными пограничной службы Беларуси в рамках “информационного обмена”<sup>44</sup>. Взаимодействие российских и белорусских силовых ведомств, включая то, что касается контроля миграции, заметно усилилось в последние годы, а в 2024 и

---

<sup>39</sup> См. статью 11 здесь: Закон РФ “О Государственной границе Российской Федерации” от 01.04.1993 N 4730-1 [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_3140/](https://www.consultant.ru/document/cons_doc_LAW_3140/) (Доступ: 18.08.2025).

<sup>40</sup> См. пункт 11 “Правил организации эксперимента” здесь: Постановление Правительства Российской Федерации от 07.11.2024 N 1510 “О проведении эксперимента по апробации правил и условий въезда в Российскую Федерацию и выезда из Российской Федерации иностранных граждан и лиц без гражданства” <https://www.garant.ru/products/ipo/prime/doc/410628090/> (Доступ: 17.08.2025).

<sup>41</sup> См. пункт 12: там же

<sup>42</sup> См. пункт 13: там же.

<sup>43</sup> Постановление Правительства РФ от 08.09.2010 N 697 (ред. от 28.11.2024) “О единой системе межведомственного электронного взаимодействия” (вместе с “Положением о единой системе межведомственного электронного взаимодействия”) [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_104665/59a1ee33e6096f0bf3fd23d27eeb41a502ed129e/#dst30](https://www.consultant.ru/document/cons_doc_LAW_104665/59a1ee33e6096f0bf3fd23d27eeb41a502ed129e/#dst30) (Доступ: 18.08.2025).

<sup>44</sup> См. подпункт “б” пункта 10, а также пункт 35 здесь: Постановление Правительства РФ от 06.08.2015 N 813 (ред. от 21.10.2024) “Об утверждении Положения о государственной системе миграционного и регистрационного учета, а также изготовления, оформления и контроля обращения документов, удостоверяющих личность” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_184040/](https://www.consultant.ru/document/cons_doc_LAW_184040/) (Доступ: 17.08.2025).

2025 году власти Беларуси и России формализовали<sup>45</sup> обмен данными о пересечении границы иностранными гражданами, а также “о выданных, аннулированных, признанных недействительными и изъятых документах, удостоверяющих личность иностранных граждан и лиц без гражданства, находящихся или проживающих на территории обоих государств”<sup>46</sup>. Это лишний раз демонстрирует как авторитарные режимы выстраивают единое пространство слежки.

Хотя российские власти обещают информировать через личный кабинет иностранного гражданина об отказах во въездах, включая основания таких отказов, однако, во-первых, такие отказы носят “справочный характер”, а, во-вторых, такое информирования касается не всех оснований<sup>47</sup>. Таким образом, даже в случае верно заполненных документов, поданного заявления на въезд, установки приложения, сдачи биометрических данных и отсутствии информации от отказе российские власти без очевидных причин и без каких-либо объяснений могут не пропустить иностранного гражданина на свою территорию.

### **3. Перемещение / система видеонаблюдения**

После того как иностранный гражданин пересекает пограничный пункт и оказывается на территории, контролируемой российскими властями, его перемещения, местонахождение и деятельность начинает отслеживаются несколькими способами и с задействованием разнообразных технологий. В этом разделе мы остановимся на теме отслеживания за передвижением с помощью видеокамер. Так, биометрические данные, которые российские власти собирают в процессе подачи документов на визу и заявления на въезд, а затем сверяются и вновь собираются на пунктах пропуска сотрудниками Пограничной службы ФСБ, среди прочего служат основой для расширения и развития систем по распознаванию лиц. Эти системы базируются на передовых технологиях, включая программы искусственного интеллекта, а также подключены к сетям видеонаблюдения, позволяя идентифицировать того или иного человека, попавшего в обзор соответствующей видеокамеры при том, что число видеокамер в последние годы быстро и постоянно увеличивается.

Начало активного выстраивания российской системы видеонаблюдения началось в Москве в 2010-х годах, сразу после того как мэром стал Сергей Собянин. Московским центром, куда стекаются и где анализируются данные с видеокамер, стал “Единый Центр Хранения Данных” (далее – ЕЦХД). Столичные власти не устают увеличивать и усовершенствовать систему видеонаблюдения, тратя на это огромные ресурсы<sup>48</sup>. По собственному признанию московских

<sup>45</sup> См. Постановление Правительства РФ от 29.08.2024 N 1180 “О внесении изменения в постановление Правительства Российской Федерации от 6 августа 2015 г. N 813” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_484735/](https://www.consultant.ru/document/cons_doc_LAW_484735/) (Доступ: 08.10.2025).

и Постановления Совета Министров Республики Беларусь от 31.03.2025 № 192 “Об информационной системе обмена сведениями”.

<sup>46</sup> Онейда, Тесса. “Россия и Беларусь подписали соглашение: будут обмениваться данными о пересечении границы.” *Belsat* (04.04.2025) <https://ru.belsat.eu/85988964/rossiya-i-belarus-obmenivayutsya-dannymi-o-pereselenii-granicy> (Доступ: 02.10.2025)

<sup>47</sup> См. Пункты 8 и 9 “Правил организации эксперимента” здесь: Постановление Правительства Российской Федерации от 07.11.2024 N 1510 “О проведении эксперимента по апробации правил и условий въезда в Российскую Федерацию и выезда из Российской Федерации иностранных граждан и лиц без гражданства” <https://www.garant.ru/products/ipo/prime/doc/410628090/> (Доступ: 17.08.2025).

<sup>48</sup> Краткий обзор истории внедрения, функционирования и применения системы видеонаблюдения в Москве см., например, Захаров, Андрей. “‘Умный город’ или ‘Старший брат’? Как мэрия научилась знать о москвичах всё”. *BBC News Русская служба* (10.04.2020) <https://www.bbc.com/russian/features-52219260> (Доступ: 15.08.2025); Легалов, Евгений. “Небольшой брат. Как видеокамеры стали инструментом репрессий”. *Радио Свобода* (07.05.2024) <https://www.svoboda.org/a/neboljshoy-brat-kak-videoekamery-stali-instrumentom-repressiy/32932369.html> (Доступ: 15.08.2025); Ковачич, Леонид. “Сделано не в Китае: как устроена система

властей в 2021-2023 годах они собирались потратить на систему видеонаблюдения 28,5 млрд рублей<sup>49</sup>. Постепенно технологии видеонаблюдения начали распространяться на другие российские регионы. В 2014 году Правительство РФ утвердило “Концепцию построения и развития аппаратно-программного комплекса ‘Безопасный город’”<sup>50</sup>. Системы видеонаблюдения (прежде всего в Москве) прошли массовый текст во время чемпионата мира по футболу 2018 года и “ковидных” ограничений 2020 года<sup>51</sup>. После успешного, как сочли чиновники, опыта Москвы и тестов в 2018 и 2020 годах российские власти решили не только более активно продвигать системы слежки в других регионах, но и создать единую центральную систему хранения и обработки данных, о чем стало известно из утечек закрытой информации<sup>52</sup>.

Оценки числа видеокамер, которые используют российские власти для слежки и контроля, варьируются. Уже на конец 2021 года, согласно экспертам TelecomDaily, в России работало 18,6 млн видеокамер, из которых 4,8 млн были настроены на распознавание лиц. В то же время, следует отметить, что это общее число видеокамер, включая видеокамеры коммерческого и частного пользования<sup>53</sup>. Что касается видеокамер, используемых непосредственно российскими властями, то тут нет точных открытых сведений. Так, в 2024 году глава Минцифры, Максут Шадаев, заявлял об одном миллионе, каждая третья из которых была подключена к системе распознавания лиц<sup>54</sup>. Значительная доля видеокамер приходится на Москву, в которой, согласно Правительству Москвы, на середину 2023 года было установлено 225 тыс. видеокамер и почти все были подключены к системам по распознаванию лиц. Однако, поскольку отсутствует независимый аудит числа видеокамер и неясно, как получены цифры, озвучиваемые чиновниками, то о реальном числе можно лишь догадываться. Например, из данных официальных порталов региональных органов власти в 2023 году следовало, что в России имеется более полумиллиона видеокамер, подключенных к системе распознавания лиц<sup>55</sup>, что значительно больше, чем то, число о котором заявил Шадаев. Кроме того, неизвестно, подразумевает ли число видеокамер, озвученное главой Минцифры, камеры, установленные и обслуживаемые российскими властями, либо это общее число камер, к которым имеют доступ российские власти. Если первое, то реальное число видеокамер, которые используют российские власти намного больше.

---

videonabлюдения Москвы”. *Московский центр Carnegie* (05.08.2020) <https://carnegie.ru/2020/08/05/ru-pub-82419> (Доступ: 15.08.2025).

<sup>49</sup> Роскомсвобода. “На столичную систему видеонаблюдения потратят порядка 28,5 млрд рублей”. (10.11.2020) <https://roskomsvoboda.org/ru/66160/> (Доступ: 22.09.2025).

<sup>50</sup> Распоряжение Правительства РФ от 03.12.2014 N 2446-р “Об утверждении Концепции построения и развития аппаратно-программного комплекса ‘Безопасный город’” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_172077/](https://www.consultant.ru/document/cons_doc_LAW_172077/) (Доступ: 15.08.2025).

<sup>51</sup> Захаров, Андрей. “‘Умный город’ или ‘Старший брат’? Как мэрия научилась знать о москвичах всё”. *BBC News Русская служба* (10.04.2020) <https://www.bbc.com/russian/features-52219260> (Доступ: 15.08.2025); Бородихин, А. “Корона доказательств. Как устроено ‘санитарное дело’”. *Медиазона* (07.07.2021) <https://zona.media/article/2021/07/07/korona-236> (Доступ: 15.08.2025).

<sup>52</sup> Дмитриев Д., Яппарова Л. “Власти задумали сделать единую систему видеонаблюдения (как в Москве, только по всей стране). Из утечки документов администрации президента мы узнали, кто ее разрабатывает.” *Медуза* (29.02.2024) <https://meduza.io/feature/2024/02/29/vlasti-zadumali-sdelat-edinyyu-sistemu-videoonablyudeniya-kak-v-moskve-tolko-po-vsey-strane-iz-utechki-dokumentov-administratsii-prezidenta-my-uznali-kto-ee-razrabatyvaet> (Доступ: 15.08.2025).

<sup>53</sup> Издание *TelecomDaily* от 30.09.2022.

<sup>54</sup> Роскомсвобода. “Каждая третья камера видеонаблюдения подключена к системам распознавания”. (12.03.2024) <https://roskomsvoboda.org/en/post/kamery-bezgorod-ai/> (Доступ: 18.08.2025)

<sup>55</sup> The Moscow Times. “Три четверти российских регионов внедрили системы слежки за гражданами”. (24.10.2023) <https://www.moscowtimes.ru/2023/10/24/tri-chetverti-rossiiskih-regionov-vnedrili-sistemi-slezhki-za-grazhdanami-a111011> (Доступ: 18.08.2025).

Для еще большего контроля российские власти предпринимают усилия для централизации систем видео слежки. Так, например, Минцифры запланировало в 2025-2026 годах создать и ввести единую федеральную систему видеонаблюдения, в которой будут направляться видеопотоки, собираемые в регионах в рамках проекта “Безопасный город”<sup>56</sup>. Камеры активно устанавливаются на пограничных пунктах, госучреждениях, магистралях, улицах, дворах, подъездах, в парках, вокзалах, аэропортах, учебных заведениях и общественном транспорте. Власти стремятся использовать обширный парк видеокамер, используемых коммерческими организациями. Согласно нормативным нововведениям, власти обязывают владельцев банков, гостиниц, магазинов, торговых центров, кафе, ресторанов иочных клубов устанавливать новые камеры и подключать имеющиеся к системам, к которым имеют свободных доступ государственные ведомства<sup>57</sup>.

Помимо увеличения числа камер, связи их с многочисленными базами данных, а также централизации сбора и аналитики данных, власти расширяют функциональность системы видеонаблюдения с помощью новых технологий, оснащенных все более изощренными алгоритмами по распознаванию лиц (например, установление личности человека даже при плохом наблюдении или если лицо значительно закрыто одеждой или медицинской маской), а также программами по идентификации людей по силуэтам и походке<sup>58</sup>. Власти также внедряют новые технологии, которые способны распознавать эмоции, этническую принадлежность, является ли человек “своим” или “чужим” в доме и поведенческие паттерны. Существует множество информационных систем и программных разработок, которые отличаются в зависимости от целей использования, ведомств и регионов, в которых они применяются<sup>59</sup>.

Внедрение систем видеослежения сопровождалось декларациями о том, что эти технологии нужны для более эффективной борьбы с преступностью и обеспечением безопасности населения. В то же время с самого начала в эти системы была заложена опция, направленная на подавление политической оппозиции, что следует даже из нормативных документов. Так, например, в федеральной концепции “Безопасного города”, среди угроз, на предотвращение которых направления эта система, среди прочего упомянуты:

- “несанкционированные публичные мероприятия”;
- “оказание целенаправленного негативного информационного воздействия на население через средства массовой информации и информационно-телекоммуникационную сеть “Интернет”;

---

<sup>56</sup> Гаврилюк, Анастасия. “Сдугая камера: Минцифры намерено создать платформу видеонаблюдения за 2 млрд рублей”. *Forbes Russia* (13.01.2025).

<sup>57</sup> См., например: Роскомсвобода. “Подключение вообще всех камер к системам Москвы – это кошмар и ужас”. (20.05.2024) <https://roskomsvoboda.org/ru/post/video-camera-coffee-shop/> (Доступ: 18.08.2025); Роскомсвобода. “Столичная мэрия заглянет в ночные клубы... через камеры видеонаблюдения”. (04.05.2022) <https://roskomsvoboda.org/en/post/podglyadet-za-nochikami/> (Доступ: 18.08.2025); The Moscow Times. “Отказаться нельзя”. Гостиницы Москвы обязали подключиться с государственной системе видеослежки за гражданами”. (19.10.2022) <https://www.moscowtimes.ru/2022/10/19/otkazatsya-nelzya-gostintsi-moskvi-obyazali-podklyuchitsya-s-gosudarstvennoi-sisteme-videoslezhki-za-grazhdanami-a25487> (Доступ: 18.08.2025); Роскомсвобода. “В Москве хотят подключить камеры ТЦ к городской системе видеонаблюдения”. (20.10.2021) <https://roskomsvoboda.org/en/post/kamery-maski-kontrol/> (Доступ: 18.08.2025).

<sup>58</sup> См., например: Гаврилюк, Анастасия. “Контрольная работа: городские камеры научат слышать звуки и распознавать силуэты”. *Forbes Russia* (13.02.2024).

<sup>59</sup> См., например: ОВД-Инфо. “Как власти используют камеры и распознавание лиц против протестующих”. 17.02.2022, <https://reports.ovd.info/kak-vlasti-ispolzuyut-kamery-i-raspoznavanie-lic-protiv-protestuyushchih> (доступ 12 августа 2025 года); Захаров, Андрей. “Злость, страх и силуэты. Мэрия Москвы раскрыла, какие алгоритмы распознают людей по лицам”. *BBC News Русская служба* (25.08.2022) <https://www.bbc.com/russian/features-62658404> (Доступ: 18.08.2025).

- “неполная реализация прав граждан в области получения и обмена достоверной информацией, в том числе манипулирование массовым сознанием с использованием информационно-психологического воздействия”;
- “провоцирование социальной, межнациональной и религиозной напряженности через деятельность отдельных (в том числе электронных) средств массовой информации”<sup>60</sup>.

Эти размытые и широкие формулировки изначально допускают злоупотребления в виде отнесения к “угрозам” любой оппозиционной акции на улице и любой критики властей в Интернете. И действительно, есть много примеров того, как российские власти активно использовали системы видеонаблюдения для борьбы с оппозицией, преследования журналистов и гражданских активистов, во время мобилизации осенью 2023 и “охоты” на призывников, а также других репрессивных целей<sup>61</sup>.

Хотя система видеонаблюдения направлена на слежку и контроль как за российскими, так и за иностранными гражданами, некоторые регионы внедряют новшества, направленные преимущественно на мигрантов. Так, например, в 2025 году Правительство Москвы обязало оборудовать все стройки системами видеонаблюдения, подключая камеры к ЕЦХД<sup>62</sup>. В феврале 2025 года власти Санкт-Петербурга открыто объявили о внедрении системы по распознаванию “этнической принадлежности” наблюдаемых людей, не скрывая, что эта система нужна им для слежки за мигрантами<sup>63</sup>. При этом, первоначально власти города сообщали о том, что этой функцией будут обладать лишь относительно небольшая доля (около восьми тысяч) действующих видеокамер (около 100 тыс.), но уже в августе 2025 года оказалось, что к этой системе подключили половину всех камер и, возможно, планируют расширять систему дальше<sup>64</sup>. Вполне вероятно, что и в других регионах, а также на федеральном уровне действуют и иные “проекты”, построенные на базе систем видеонаблюдения и направленные именно или преимущественно на слежку за иностранными гражданами.

То, что системы распознавания лиц используются российскими властями в том числе для того, чтобы задерживать тех иностранных граждан, кого они считают “нелегально” находящимися в России, известно уже несколько лет. Еще в 2020 году в МВД заявляли, что начинают

<sup>60</sup> Распоряжение Правительства РФ от 03.12.2014 N 2446-р “Об утверждении Концепции построения и развития аппаратно-программного комплекса ‘Безопасный город’” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_172077/](https://www.consultant.ru/document/cons_doc_LAW_172077/) (Доступ: 15.08.2025).

<sup>61</sup> См., например: ОВД-Инфо. “Как власти используют камеры и распознавание лиц против протестующих”. (17.02.2022) <https://reports.ovd.info/kak-vlasti-ispolzuyut-kamery-i-raspoznavanie-lic-protiv-protestuyushchih> (доступ 12 августа 2025 года); ОВД-Инфо и Роскосвобода. “Права человека и новые технологии в России”. (06.03.2023) <https://reports.ovd.info/prava-cheloveka-i-novye-tehnologii-v-rossii> (доступ 8 августа 2025 года); Литвин, В. “Достали из бани”. *Новая Газета Европа*, (15.08.2024) <https://novayagazeta.eu/articles/2024/08/15/dostali-iz-bani> (Доступ: 19.08.2025); International Partnership for Human Rights (IPHR) and Global Diligence LLP. “Russia’s Digital Authoritarianism: the Kremlin’s Toolkit”. September, 2023 <https://iphronline.org/articles/russias-digital-authoritarianism-the-kremlins-toolkit/> (accessed August 12, 2025); Human Rights Watch. “Disrupted, Throttled, and Blocked State Censorship, Control, and Increasing Isolation of Internet Users in Russia”. July, 2025 [https://www.hrw.org/sites/default/files/media\\_2025/07/russia0725%20web.pdf](https://www.hrw.org/sites/default/files/media_2025/07/russia0725%20web.pdf) (accessed August 8, 2025); Soldatov, A., Borogan, I. “Digital Surveillance and the Impact on Journalism in Russia”. *Friedrich Naumann Foundation for Freedom*, (2020) <https://shop.freiheit.org/#!/Publikation/943> (accessed August 18, 2025).

<sup>62</sup> Постановление Правительства Москвы от 21.01.2025 N 47-ПП “О внесении изменений в постановления Правительства Москвы от 16 июня 2011 г. N 272-ПП и от 19 мая 2015 г. N 299-ПП” <https://www.consultant.ru/law/review/209259861.html> (Доступ: 18.08.2025).

<sup>63</sup> Радио Свобода. Idel.Реалии. “Камеры в Санкт-Петербурге начнут распознавать ‘этническую идентичность’, чтобы следить за мигрантами”. (20.02.2025) <https://www.idlreal.org/a/kamery-v-peterburge-nastroyat-na-raspoznavanie-etnosa/33321484.html> (Доступ: 19.08.2025).

<sup>64</sup> Роскомсвобода. “Петербургские видеокамеры научили распознавать этническую принадлежность”. (25.08.2025) <https://roskomsvoboda.org/ru/post/ethnicity-detection-cctv-russia-policy/> (Доступ: 26.09.2025).

использовать технологии искусственного интеллекта для выявления таких мигрантов. В качестве примера можно упомянуть одну из последних крупных операций в Москве, когда, судя по всему, при помощи государственной автоматизированной информационной системы “Сфера” (далее – ГАИС Сфера)<sup>65</sup>, которая используется сотрудниками МВД в московском метрополитене, массово задерживались иностранные граждане, подозреваемые в нарушении миграционных норм<sup>66</sup>. Примечательно, что ранее российские силовые ведомства использовали систему ГАИС Сфера для превентивных задержаний журналистов, гражданских активистов и оппозиционеров<sup>67</sup>.

Слежка за физическим перемещением с помощью систем видеонаблюдения тесно переплетена со слежкой в Интернете. Так, например, фотографии высокого качества, который иностранный гражданин сдал для получения визы или при подаче заявления на въезд, помогают российским властям не только обнаруживать его на улицах, в общественном транспорте и в зданиях, но и идентифицировать его в социальных сетях, а также на выкладываемых в Интернете изображениях и видео. Этот процесс действует и в обратном направлении, то есть когда людей, изображенных на фото или видео, выложенных в Интернет, обнаруживают в системе видеонаблюдения. Поэтому, хотя ради удобства изложения можно различать систему видеонаблюдения и слежку в Интернете, но границы часто размыты и по сути речь идет о тесно связанных между собой элементов единой и более общей системы слежки.

#### **4. Пользование телефоном и Интернетом / мониторинг и цензура**

После пересечения российский пограничных пунктов иностранный гражданин: Во-первых, лишается или ограничивается в доступе или в функционале ко многим иностранным социальным платформам и новостным сайтам в связи с признанием их российскими властями “нежелательными” или “экстремистскими”. Во-вторых, российские системы начинают отслеживать то, что иностранного гражданина делает в Интернете. В-третьих, иностранный гражданин оказывается под риском быть привлеченным к административной или уголовной ответственности за ряд действий в Интернете<sup>68</sup>, к которым совсем недавно российские власти прибавили административное наказание за поиск и ознакомление с материалами, которые они рассматривают как “экстремистские”<sup>69</sup>. Не удивительно, что, согласно рейтингу “Свобода в сети 2024” (Freedom On the Net 2024), среди 72 стран, включенных в рейтинг, Российская Федерация отмечена как несвободная и делит с Кубой четвертое-пятое места от конца (ниже расположились лишь Китай, Мьянмар и Иран)<sup>70</sup>.

---

<sup>65</sup> Постановление Правительства Москвы от 17.03.2021 N 328-ПП “О государственной автоматизированной информационной системе ‘Сфера’” <https://base.garant.ru/400484831/> (Доступ: 23.08.2025).

<sup>66</sup> Мемориал: Центр Защиты Прав Человека. “Задержания мигрантов в Москве: комментарии юристов”. (19.06.2024) <https://memorialcenter.org/ru/news/zaderzhaniya-migrantov-v-moskve-komentarii-yuristov-1> (Доступ: 19.08.2025).

<sup>67</sup> См., например, рассказ об использовании ГАИС Сфера при нескольких десятках превентивных задержаний весной 2022 года здесь: Издание “Бумага”. “Как оппозиционеров задерживают с помощью распознавания лиц. Рассказываем о московской системе ‘Сфера’ и ее аналоге в Петербурге”. 15.06.2022 <https://paperpaper.io/kak-oppozicionerov-zaderzhivayut-s-pom/> (Доступ: 21.08.2025).

<sup>68</sup> См., например: Human Rights Watch. “Disrupted, Throttled, and Blocked State Censorship, Control, and Increasing Isolation of Internet Users in Russia”. July, 2025, [https://www.hrw.org/sites/default/files/media\\_2025/07/russia0725%20web.pdf](https://www.hrw.org/sites/default/files/media_2025/07/russia0725%20web.pdf) (accessed August 8, 2025).

<sup>69</sup> Дик, С.; Тихомирова, О. “Наказание за поиск в Сети. Какие штрафы грозят россиянам”. Deutsche Welle (23.07.2025) <https://www.dw.com/ru/nakazanie-za-poisk-v-internete-kakie-strafy-grozat-rossianam/a-73388354> (Доступ: 19.08.2025).

<sup>70</sup> Freedom House. “Freedom On the Net 2024”. October 2024, <https://freedomhouse.org/sites/default/files/2024-10/FREEDOM-ON-THE-NET-2024-DIGITAL-BOOKLET.pdf> (accessed October 3, 2025).

Слежка и контроль в телефонии и Интернете во многом осуществляется российскими властями посредством Системы оперативно-розыскных мероприятий (далее – СОРМ), которая представляет собой совокупность организационных, нормативных и технологических инструментов, позволяющих отслеживать, хранить и анализировать данные, собираемые из телефонного и интернет трафика. ФСБ внедряет и контролирует СОРМ, история разработки которой началась еще в недрах КГБ. В 1990-х годах СОРМ был в основном предназначен для прослушки телефонных разговоров. Вскоре к этому добавилась слежка в Интернете, которая постепенно стала очень замысловато и почти тотальной. Уже много лет и не особо скрывая ФСБ занято контролем интернет-трафика, что проявляется в частности в обязательном установлении оборудования СОРМ и физическом присутствии сотрудников этой спецслужбы в точках обмена интернет-трафиком в России<sup>71</sup>.

Постепенно власти обязали внедрять и участвовать в системе СОРМ всех операторов связи, провайдеров и даже российские интернет-сервисы (форумы, социальные сети, блоги), занимающихся обслуживанием населения в области телефонной и интернет связи<sup>72</sup>. Власти не остановило то, что еще в 2015 году Европейский суд по правам человека признал систему СОРМ открытой для злоупотреблений и не соответствующей требованиям Европейской конвенции по правам человека (см. *Zakharov v. Russia*). Наоборот, с тех пор российские власти усилили и расширили действие системы. Важным пунктом по расширению полномочий спецслужб и усовершенствованию системы слежки было принятие так называемого “закона Яровой” (ФЗ от 06.07.2016 N 374-ФЗ<sup>73</sup> и ФЗ от 06.07.2016 N 375-ФЗ<sup>74</sup>), причем затраты, связанные со слежкой за пользователями, были в основном возложены на компании (например, хранение в течение 30 дней всего интернет-трафика и в течение полугода данных о фактах соединения). За прошедшие с тех поры годы российские власти приняли ряд других нормативных актов, направленных на расширение, углубление о облегчение слежки за пользователями Интернета. При этом, если какая-то компания отказывается от тесного сотрудничества со спецслужбами, то у нее, как правило, быстро находят различные “нарушения” и в случае упорства она лишается лицензии. Как итог, российские мобильные операторы, интернет-провайдеры, интернет-сервисы и хранилища данных тесно связаны со спецслужбами, которые имеют круглосуточный и фактически неограниченный доступ к данным этих компаний<sup>75</sup>. В качестве одного из инструментов для принуждения к слежке российские власти используют так называемый “Реестр организаторов распространения

---

<sup>71</sup> Подробно об истории СОРМ см., например: Солдатов, Андрей и Ирина Бороган. *Битва за Рунет: Как власть манипулирует информацией и следит за каждым из нас*. Москва, Альпина Паблишер, 2017.

<sup>72</sup> Постановление Правительства РФ от 31.07.2014 N 743 “Об утверждении Правил взаимодействия организаторов распространения информации в информационно-телекоммуникационной сети ‘Интернет’ с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации” <https://base.garant.ru/70709018/> (Доступ: 19.08.2025).

<sup>73</sup> Федеральный закон “О внесении изменений в Федеральный закон ‘О противодействии терроризму’ и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности” от 06.07.2016 N 374-ФЗ [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_201078/](https://www.consultant.ru/document/cons_doc_LAW_201078/) (Доступ: 19.08.2025).

<sup>74</sup> Федеральный закон “О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности” от 06.07.2016 N 375-ФЗ [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_201087/](https://www.consultant.ru/document/cons_doc_LAW_201087/) (Доступ: 19.08.2025).

<sup>75</sup> Позычанюк, В.; Мироненко, П. “ФСБ потребовала от интернет-сервисов онлайн-доступ к данным и переписке пользователей”. *The Bell* (11.02.2020) <https://thebell.io/fsb-potrebovala-ot-internet-servisov-onlajn-dostup-k-dannym-i-perepiske-polzovatelei> (Доступ: 19.08.2025).

информации” (далее – Реестр ОРИ)<sup>76</sup>. Тот, кто попадает в Реестр ОРИ, власти обязывают делиться фактически всей информацией с силовыми ведомствами.

Как видно из последних новостей, российские власти решили не ограничиваться тем, что силовые ведомства имеют открытый и фактически неограниченный доступ к данным операторов связи, провайдеров и владельцам сайтов, а взяли курс на активное понуждение последних самим также осуществлять слежку и сообщать о “признаках правонарушений”<sup>77</sup>.

Слежка в Интернете также осуществляется в рамках концепции так называемого “суверенного интернета”. Главным координатором внедрения этой концепции является Роскомнадзор и особенно две его структурных единицы: “Главный радиочастотный центр” (ФГУП “ГРЧЦ”) и “Центр мониторинга и управления сетью связи общего пользования” (ЦМУ “ССОП”)<sup>78</sup>. Именно Роскомнадзор занимается массовыми блокировками сайтов, ограничением трафика, замедлением скорости платформ, отказывающихся сотрудничать с российскими системами, а также выстраиванием так называемого “российского сегмента Интернета”, главными принципами которого является егоозвучие официальной пропаганде, а также подконтрольность для Роскомнадзора и силовых служб<sup>79</sup>.

Особо следует коснуться слежки в социальных сетях и мессенджерах. Не секрет, что российские социальные сети и мессенджеры тесно сотрудничают с российскими властями и обычно совершенно прозрачны для спецслужб. Что касается иностранных социальных сетей и мессенджеров, то в отношении них власти используют три основных инструмента:

1. Выдавливание или прямой запрет на деятельность (так, например, в России были заблокированы или частично ограничены такие популярные мессенджеры и социальные сети, как Whatsapp, Signal, Linkedin, Discord, Viber, Telegram, Facebook, Instagram, X);
2. Давление с целью добиться сотрудничества (так, например, особо известна история давления российских властей на мессенджер и социальную сеть Telegram даже при том, что журналисты нашли косвенные свидетельства о возможном наличии у российских спецслужб доступа к переписке пользователей Telegram<sup>80</sup>);
3. Изобретение и использование технологий и вредоносных программ, позволяющих получать несанкционированный доступ к конфиденциальной переписке и данным (так, согласно

---

<sup>76</sup> Федеральный закон от 05.05.2014 N 97-ФЗ “О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_162586/](https://www.consultant.ru/document/cons_doc_LAW_162586/) (Доступ: 05.09.2025).

<sup>77</sup> Коржова, Дарья. “Самозапреты и отключения: власти запланировали меры по защите граждан в интернете”, *Forbes Russia* (21.08.2025).

<sup>78</sup> Постановление Правительства РФ от 13 февраля 2019 г. N 136 "О Центре мониторинга и управления сетью связи общего пользования" см. здесь: <https://base.garant.ru/72180742/> (доступ 14.08.2025). Приказ Роскомнадзора от 31.07.2019 N 225 (ред. от 24.04.2024) "Об утверждении Положения о Центре мониторинга и управления сетью связи общего пользования" см. здесь: [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_338375/5ca8c9d8a91fec8a0bb0794025b7f411b9b705f8/](https://www.consultant.ru/document/cons_doc_LAW_338375/5ca8c9d8a91fec8a0bb0794025b7f411b9b705f8/) (доступ 14.08.2025).

<sup>79</sup> Подробнее о концепции и первых годах внедрении “суверенного интернета” в России см., например: Epifanova, Alena. “Deciphering Russia’s ‘Sovereign Internet Law.’ Tightening Control and Accelerating the Splinternet”. *German Council on Foreign Relations*. January 2020. [https://dgap.org/sites/default/files/article\\_pdfs/dgap-analyse\\_2020\\_epifanova\\_0.pdf](https://dgap.org/sites/default/files/article_pdfs/dgap-analyse_2020_epifanova_0.pdf) (accessed August 14, 2025) и Soldatov, Andrei and Irina Borogan. “The New Iron Curtain”. *The Center for European Policy Analysis* (CEPA). June 7, 2022 <https://cepa.org/comprehensive-reports/the-new-iron-curtain-2/> (accessed August 14, 2025).

<sup>80</sup> Кагермазов, С.; Попова, А. “Не самый надежный мессенджер? Основные вопросы о Telegram.” *BBC News Русская служба* (11.06.2025) <https://www.bbc.com/russian/articles/c0lndgzw1o> (Доступ: 19.08.2025).

экспертом, российские спецслужбы используют разнообразные программы слежки, позволяющие взламывать и обходить защиту известных иностранных мессенджеров<sup>81</sup>).

Как лишний раз продемонстрировала блокировка Whatsapp, российские власти в общем нацелены на исключение всех западных компаний телекоммуникационных и интернет компаний с заменой иностранных социальных сетей и мессенджеров российскими “аналогами”, которые полностью контролируются людьми, аффилированными с властями и являются прозрачными для силовых ведомств.

Самой популярной российской социальной сетью как среди российских граждан, так и трудовых мигрантов является ВКонтакте (около 90 млн пользователей в месяц). ВКонтакте принадлежит холдингу VK, в который кроме того входит социальная сеть Одноклассники (также популярная среди мигрантов), почтовый сервис Почта Mail, платформа блогов и новостей Дзен, сервис объявлений Юла, сервис Учи.ру и другие интернет сервисы и площадки. При этом холдинг VK – центральный элемент в системе слежки на интернет платформах и мессенджерах, выстраиваемой российскими властями. Не случайно, что в 2021 году компания перешла под прямое управление государства (управляющая доля компании была выкуплена Газпромом), а генеральным директором стал Владимир Кириленко (сын руководителя кремлевской администрации)<sup>82</sup>. Не удивительно, что сервисы платформы VK особо активно используются российскими властями для слежки, преследований, манипуляций, дезинформации и троллинга<sup>83</sup>.

Также не вызывает удивления, что именно в рамках холдинга VK российские власти решили создать замену мессенджеру Whatsapp, руководство которого не соглашалось предоставлять все данные российскими властям. Уже давно российские компании предпринимали попытки создания “отечественного” мессенджера, но успеха добиться не могли и Whatsapp оставался самой популярной программой среди российских пользователей. Ситуация поменялась в середине 2025 году в результате прямого вмешательства государственных ведомств. Так, в 2025 году компания VK закончила разработку мессенджера Макс, который был тут же утвержден Правительством РФ как “национальный российский мессенджер” и начал активно внедряться с помощью государственных рычагов давления. Параллельно этому началась активная пропагандистская медиа кампания против Whatsapp и замедление его работы российскими властями, которые тем самым стремятся понудить пользователей переходить на мессенджер Макс.

При этом, даже из Политики конфиденциальности мессенджера Макс следует, что он не только собирает данные о местоположении, браузере, установленных приложениях, контактах, номере IP, всех действиях в сервисе, но и на свое усмотрение передает эти данные третьим лицам, включая государственные ведомства. И это лишь из того, что разработчики

---

<sup>81</sup> Krolik, A.; Mozur, P.; Satariano, A. “Cracking Down on Dissent, Russia Seeds a Surveillance Supply Chain”. *The New York Times* (03.07.2023) <https://www.nytimes.com/2023/07/03/technology/russia-ukraine-surveillance-tech.html> (accessed August 19, 2025).

<sup>82</sup> Медуза. “VK перешел под контроль Газпромбанка и «Согаза» друга Путина Юрия Ковалчука. Гендиректором VK станет сын Сергея Кириенко”. (03.12.2021) <https://meduza.io/feature/2021/12/03/vk-pereshel-pod-kontrol-gazprombanka-i-sogaza-druga-putina-yuriya-kovalchuka-gendirektorom-vk-stanet-syn-sergeya-kirienko> (Доступ: 23.08.2025).

<sup>83</sup> См., например: Dietrich, P. “The Key Player in Russia’s Cybersphere. What the West Needs to Know about VK Company”. *German Council on Foreign Relations* (20.09.2023) <https://dgap.org/en/research/publications/key-player-russias-cybersphere> (accessed August 19, 2025).

мессенджера прямо признают<sup>84</sup>. Нельзя исключить, что программа имеет и неафишированный функционал, например, чтения паролей, неавторизованное подключение к микрофону и камере, доступ к снимкам экрана и тому подобное. Бросается также в глаза, что в отличие, например, от Whatsapp в мессенджере Max отсутствует сквозное шифрование, а система шифровки разрабатывалась в ФСБ<sup>85</sup>. Все это роднит мессенджер Max с китайским аналогом WeChat, известным своей полной прозрачностью китайским властям и давно использующимся в качестве инструмента слежки, пропаганды, контроля, преследования и цензуры<sup>86</sup>. Российские власти даже не скрывают и указывали, что одним из примеров для мессенджера Max, является именно его китайский аналог и так заинтересованы во внедрении удобного инструмента для слежки, что с сентября 2025 года обязали переустанавливать Max на все смартфоны<sup>87</sup>.

Хотя “российский сегмент” Интернета пока не изолирован полностью от “мировой сети”, очевидно, что власти активно готовятся к этому. Так, об этих намерениях свидетельствует не только выдавливание последних оставшихся западных компаний и сервисов, но и регулярные отключения интернета, стремительное увеличение числа уже заблокированных сайтов, а также публичные тестирования отключения от “мировой сети”<sup>88</sup>.

Помимо сохраняющейся пока связи с “мировой паутиной” несколько затрудняет слежку, особенно то, что касается мобильного интернета и телефонии, широкий оборот на рынке обезличенных СИМ-карт. Не удивительно, что российские чиновники решили принять новые нормы, направленные против этого обхода слежки при том, что некоторые нормы направлены именно на иностранных граждан. Так, согласно новому закону, с 1 января 2025 года иностранный гражданин может заключить договор связи исключительно очно и в салоне связи, а СИМ-карта прикрепляется к конкретному мобильному устройству через указания IMEI (的独特的 международный номер мобильного устройства). Кроме того, помимо удостоверения личности при заключении договора от иностранного гражданина требуется указать СНИЛС, учетную запись на ЕПГУ (портале “Госуслуг”), зарегистрироваться и пройти процедуру подтверждения биометрии в ЕБС. При этом, согласно поправкам в закон “О связи” от 2024 года, последнее действует также для тех, кто заключил договор ранее<sup>89</sup>. Согласно властям, на начало лета 2025 год свою биометрию для пользования российской мобильной

<sup>84</sup> The Insider. “VK представила ‘российский WeChat’: приложение получает доступ к микрофону, камере и передает данные властям. Главное о мессенджере”. <https://theins.ru/news/281890> (05.06.2025) (Доступ: 20.08.2025).

<sup>85</sup> Александров, А. “В России начали широко рекламировать мессенджер Max. В чем его опасность и способен ли он стать аналогом китайского WeChat?” *Настоящее время* (14.07.2025) <https://www.currenttime.tv/a/v-rossii-nachali-shiroko-reklamirovat-messendzher-max-v-chem-ego-opasnost-i-sposoben-li-on-stat-analogom-kitayskogo-wechat-/33472932.html> (Доступ: 21.10.2025).

<sup>86</sup> Kócsi, B.; Finn, B. “Investigating WeChat: An introduction to social apps WeChat and Weixin”. *Reporters Without Borders* (12.08.2024) <https://safety.rsf.org/investigating-wechat-an-introduction-to-social-apps-wechat-and-weixin/> (accessed August 20, 2025).

<sup>87</sup> Медуза. “Мессенджер Max начнут предустанавливать на все смартфоны в России с 1 сентября.” (21.08.2025) <https://meduza.io/news/2025/08/21/messendzher-max-stanut-predustanavlivat-na-vse-smartfony-v-rossii-s-1-sentyabrya> (Доступ: 21.08.2025).

<sup>88</sup> См., например: Глухова, Н.; Борисенко, Л. “Где и как в России отключают интернет”. *Новая газета Европа* (08.07.2025) <https://novayagazeta.eu/articles/2025/07/08/gde-i-kak-v-rossii-otkliuchaiut-internet> (Доступ: 20.08.2025); Шестаков, К. “В РФ проводят учения по отключению от зарубежного интернета”. *Detusche Welle* (06.12.2024) <https://www.dw.com/ru/v-rossii-provoda-ucenia-po-otkluceniu-ot-zarubeznogo-interneta/a-70989516> (Доступ: 20.08.2025); Редакция “Вёрстка”. “Власти ограничили доступ к рекордному числу сайтов в 2024 году — более чем к 417 тысячам”. *Вёрстка* (28.01.2025) <https://verstka.media/vlasti-ogranichili-dostup-k-rekordnomu-chislu-saitov-v-2024-godu-bolee-chem-k-417k-news> (Доступ: 20.08.2025).

<sup>89</sup> Федеральный закон от 08.08.2024 N 303-ФЗ “О внесении изменений в Федеральный закон ‘О связи’ и отдельные законодательные акты Российской Федерации” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_482565/](https://www.consultant.ru/document/cons_doc_LAW_482565/) (Доступ: 20.08.2025).

связью сдали 2 млн иностранных граждан<sup>90</sup>. С 1 июля 2025 года операторы мобильной связи начали отключать предоставление своих услуг тем иностранным гражданам, которые не выполнили этих новых требований властей<sup>91</sup>.

Российским властям показалось недостаточно документально и технически прикрепить отдельный телефонный номер и мобильное устройство к конкретному человеку, для них крайне важно, чтобы этот человек с этим устройством не расставался. Вероятно, поэтому 1 апреля 2025 года российские власти приняли Федеральный закон N 41-ФЗ “О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации”. Этим законом российские власти расширяют полномочия силовых ведомств, включая доступ к банковской информации, но главное с учетом темы нашего обзора, что с 1 сентября 2025 года вводится запрет на передачу мобильных телефонов и СИМ-карт другим людям (за исключением родственников и отдельных экстренных случаев)<sup>92</sup>.

В связи с темой миграции важно также указать, что российские власти занимаются экспортом своих систем и оборудования на Кубу, Венесуэлу, а также в Беларусь и страны Центральной Азии (Узбекистан, Киргизстан и Казахстан) и, как отмечено в докладе компании Recorded Future, занимающейся кибербезопасностью, российские спецслужбы, вероятно, сохраняют доступ к этим экспортируемым системам<sup>93</sup>.

## 5. Общение/распознавание речи

Помимо фотографий с недавних порой российские власти сильно озабочились сбором с мигрантов “образцов голоса”. В связи с этим требуется упомянуть про технологии распознавания речи, которые получают все большее распространение в России.

Современные технологии позволяют с высокой точностью идентифицировать человека по голосу для чего, разумеется, необходимо иметь в базе данных образец голоса для сравнения. Стремлением власти собрать как можно больше этих образцов, видимо, объясняется, почему в 2018 году банкам в России было разрешено внедрять технологии идентификации по голосу. Это разрешение “совпало” с запуском государственной ЕБС, куда банки начали направлять биометрические данные своих клиентов<sup>94</sup>. Хотя формально от банков требуется получить согласие на такую передачу, однако по факту нельзя исключить, что в ЕБС попали все или большинство собранных образцов голоса<sup>95</sup>. Примечательно, что среди первых опцию распознавания по голосу стали использовать такие гиганты, как Сбербанк, ВТБ, Газпромбанк,

<sup>90</sup> Рофе, Ж. “Иностранцев в РФ, не сдавших биометрию, лишат сим-карт”. *Deutsche Welle* (01.07.2025) <https://www.dw.com/ru/inostranev-v-rossii-ne-sdavshih-biometriu-lisat-simkart/a-73109351> (Доступ: 20.08.2025).

<sup>91</sup> Там же..

<sup>92</sup> Федеральный закон от 01.04.2025 N 41-ФЗ “О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_502182/](https://www.consultant.ru/document/cons_doc_LAW_502182/) (Доступ: 20.08.2025).

<sup>93</sup> Insikt Group. “Tracking Deployment of Russian Surveillance Technologies in Central Asia and Latin America”. (07.01.2025) <https://go.recordedfuture.com/hubfs/reports/ta-ru-2025-0107.pdf> (accessed August 20, 2025).

<sup>94</sup> Федеральный закон от 31.12.2017 № 482-ФЗ “О внесении изменений в отдельные законодательные акты Российской Федерации” <https://www.garant.ru/products/ipo/prime/doc/71748784/> (Доступ: 20.08.2025).

<sup>95</sup> Дульнева, М. “‘Тинькофф’ и Сбербанк теперь передают биометрические данные клиентов властям. Чем опасно хранение таких данных в государственной системе — и как запретить их использовать?” *Медуза* (12.10.2023) <https://meduza.io/cards/tinkoff-i-sberbank-teper-peredayut-biometricheskie-dannye-klientov-vlastyam-chem-opasno-hranenie-takih-dannyh-v-gosudarstvennoy-sisteme-i-kak-zapretit-ih-ispolzovat> (Доступ: 20.08.2025).

Россельхозбанк и Почта банк, то есть банки, контрольный пакет акций которых принадлежит государству.

Технологии распознавания по голосу также были внедрены в портал Госуслуг (ЕПГУ), в сети МФЦ и даже в сервисы Почты России. Так, иностранному гражданину, который захочет воспользоваться ЕПГУ (порталом “Госуслуг”) или посетить МФЦ, вполне вероятно предложат записать образец голоса (нельзя исключить, что в некоторых случаях запись сделают и без просьбы о разрешении), который попадет в ЕБС, где они становятся доступны многочисленным государственным ведомствам. Наряду с этим в декабре 2022 года российские власти приняли закон “Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных”, согласно которому МФЦ, также как ряд других государственных, муниципальных и частных организаций, обязаны передавать биометрические данные в государственную систему (ЕБС)<sup>96</sup>.

В целом возможностей у иностранного гражданина избегнуть направления своего образца голоса в государственной ЕБС все меньше. Как указывалось, с 1 июля 2025 года российские операторы связи стали требовать в обязательном порядке наличия подтвержденных биометрических данных, в который входит образец голоса, в качестве условия для начала или продолжения оказания услуг. Цель всего этого, очевидно, заключается в том, чтобы любой иностранный гражданин, пребывающий в России, мог быть идентифицирован не только через видео и фотосъемку, но и по голосу, что облегчает спецслужбам прослушку телефонных разговоров, голосовых сообщений, а также слежку в любом месте, где ведется соответствующая голосовая запись (МФЦ, офисы многих банков и государственных ведомств, консультации по телефону и т.д.).

Существует ряд российский компаний, занимающихся разработками технологий по распознаванию голоса (например, Yandex, Инлексис, ДСС Лаб, Клерити, Naumen, АСМ Решения). Здесь следует упомянуть, вероятно, наиболее важную для российский властей, которая к тому же фактические принадлежит государству. Речь идет о компании “Центр речевых технологий” (ЦРТ). Эта компания была основана в 1990 году на базе разработок, находящихся под контролем КГБ<sup>97</sup>, а с 2019 года принадлежит Сбербанку (до этого Газпромбанку). У компании целый ряд продуктов, среди которых AgentNavigator (создание ИИ агентов, в том числе распознающих голос), программа “Чарли” (распознавание речи и преобразование ее в текст), Voice2Med (программа по преобразованию в текст озвученных медицинским персоналом документов). Особое внимание вызывает платформа VoiceKey, куда, например, входит программа для сбора биометрических данных VoiceKey.INSPECTOR, интегрированная с ЕБС. Среди клиентов ЦРТ давно присутствуют многие центральные государственные органы, включая силовые ведомства<sup>98</sup>.

---

<sup>96</sup> Федеральный закон “Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации” от 29.12.2022 N 572-ФЗ [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_436110/](https://www.consultant.ru/document/cons_doc_LAW_436110/) (Доступ: 20.08.2025).

<sup>97</sup> См., например: Солдатов, Андрей и Ирина Бороган. *Битва за Рунет: Как власть манипулирует информацией и следит за каждым из нас*. Москва, Альпина Паблишер, 2017.

<sup>98</sup> См., например: Легезо, Д. “ЦРТ разработает в Сколково биометрическую систему для силовиков”. *Cnews* (18.07.2011), а также Солдатов, Андрей и Ирина Бороган. *Битва за Рунет: Как власть манипулирует информацией и следит за каждым из нас*. Москва, Альпина Паблишер. 2017.

## **6. Пользование транспортом и услугами гостиничного комплекса / проверки и отслеживание передвижения**

Гостиницы, хостелы, санатории и другие организации, принадлежащие к гостиничному бизнесу, фиксируют прибытие и убытие иностранного гражданина, а также ставят его на миграционный учет. До недавнего времени организации гостиничного бизнеса передавали данные об иностранных гражданах, воспользовавшихся их услугами, в МВД через разнообразные программы (например, АИС “ЭЛПОСТ”, СБИС (Saby), Скала-гостиница, Контур.ФМС). Однако, с 2024 года, видимо, стремясь к централизации и унификации потока данных, российские власти реализовали эту функцию на базе ЕПГУ, устранив программы “посредники”. Российские власти обязывают организации гостиничного бизнеса передавать в течение одного рабочего дня уведомление как о “прибытии”, так и о “убытии” иностранного гражданина.

Так, уведомление о прибытии включает персональные данные (ФИО, дата и место рождения, пол, гражданство), место регистрации, период пребывания, а также номер и серию паспорта. К уведомлению гостиницы прикладывают копию паспорта и миграционной карты. Понятно, что доступ к данным иностранных граждан, остановившихся в организациях российского гостиничного бизнеса, помимо МВД имеют и многие другие ведомства через ЕСМЭВ.

Помимо этого, власти внедрили в организациях российских гостиничного бизнеса регистрацию в гостинице через ЕСИА, что позволяет моментально фиксировать всех постояльцев и вместе тем собирать биометрические данные. Московские власти пошли еще дальше и в 2022 году настоятельно “порекомендовали”, а по сути обязали гостиницы и хостелы подключить свои системы видеонаблюдения к государственному ЕЦХД<sup>99</sup>.

Уже давно в России для покупки билета и посадки на поезд дальнего следования необходимо заполнить анкету и предъявить документ, удостоверяющий личность. В целом это широко распространенная в мире практика. Несколько менее распространена, хотя в России используется в обязательном порядке, это практика по установке систем видеонаблюдения непосредственно в каждом вагоне, а также объем и детальность собираемых данных<sup>100</sup>. По аналогии с регистрацией в гостинице в 2025 году была также внедрена практика по биометрической идентификации при покупке и посадки на поезда. Хотя, некоторые пользователи находят это удобным, в то же время такая система, разумеется, облегчает слежку<sup>101</sup>.

Установка видеокамер касается также междугородних автобусов, а информация о передвижении российских и иностранных граждан стекается в “автоматизированные централизованные базы персональных данных о пассажирах и персонале (экипаже)

---

<sup>99</sup> The Moscow Times. ““Отказаться нельзя”. Гостиницы Москвы обязали подключиться с государственной системе видеослежки за гражданами”. (19.10.2022) <https://www.moscowtimes.ru/2022/10/19/otkazatsya-nelzya-gostintsi-moskvi-obyazali-podklyuchitsya-s-gosudarstvennoi-sisteme-videoslezhki-za-grazhdanami-a25487> (Доступ: 18.08.2025).

<sup>100</sup> Постановление Правительства РФ от 26.09.2016 N 969 “Об утверждении требований к функциональным свойствам технических средств обеспечения транспортной безопасности и Правил обязательной сертификации технических средств обеспечения транспортной безопасности” <https://base.garant.ru/71500596/> (Доступ: 24.08.2025).

<sup>101</sup> Постановление Правительства РФ от 13.02.2025 N 156 “О внесении изменений в постановление Правительства Российской Федерации от 27 мая 2021 г. N 810” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_499251/](https://www.consultant.ru/document/cons_doc_LAW_499251/) (Доступ: 24.08.2025).

транспортных средств” (АЦБПДП), которые включаются в состав единой государственной информационной системы обеспечения транспортной безопасности (ЕГИС ОТБ)<sup>102</sup>.

Все менее анонимным становится и пользование общественным городским транспортом. Метро крупнейших городов наполнено камерами, включая скрытые. В Москве помимо тоннелей, перронов, вестибюлей, камеры находятся и в каждом вагоне поезда. Также, камеры устанавливаются в обязательном порядке в автобусы и трамваи. Столичная практика постепенно распространяется и на другие российские города города.

Не упускают из своего внимания российские власти слежку за пассажирами такси. Так, заказ такси обычно осуществляется через российские сервисы и приложения, которые делятся с силовыми ведомствами данными о своих пользователях<sup>103</sup>. Этого некоторым российским политикам показалось недостаточным и в конце 2024 года в Госдуме появился законопроект об обязательной установке видеокамер во всех салонах такси<sup>104</sup>. Хотя законопроект не был принят, однако он с очевидностью демонстрирует установку на тотальную слежку, а салоны многих такси и без этого уже оснащены камерами.

В услуги каршеринга и даже просто заправки также все больше опутывают системы государственной слежки. Известно, например, что сервис “Яндекс.Драйв”, позволяющий арендовать автомобили и сервис “Яндекс.Заправки”, позволяющий оплачивать заправки, в 2024 году были включены в реестр ОРИ, то есть тех, кто обязан беспрепятственно и по первому требованию делиться информацией о своих пользователях с силовыми ведомствами<sup>105</sup>. Сервис “Яндекс.Микромобильность”, позволяющий арендовать самокаты и велосипеды, попал в реестр ОРИ даже раньше – в 2022 году<sup>106</sup>. Есть высокая вероятность того, что российские власти и особенно силовые ведомства в рутинном порядке отслеживают пользователей и других российских сервисов.

Кроме того, в Москве 1 сентября 2025 года было введено требование для пользователей каршеринга регистрироваться и проходить верификацию на Официальном портале мэра и правительства Москвы через систему аутентификации и регистрации для доступа к цифровым ресурсам города MOS ID (далее – MOS ID), что выводит государственную слежку за пользователями каршеринга на новый уровень. Следует отметить, что ранее в 2025 году требования подобной регистрации и верификации через MOS ID были введены для тех, кто арендует в Москве электросамокаты и велосипеды<sup>107</sup>.

В целом передвижения автомобилей отслеживают десятки тысяч дорожных видеокамер, которые подключены к централизованной информационно-аналитической системе ГИБДД

---

<sup>102</sup> Приказ Минтранса России от 02.05.2024 N 162 “Об утверждении порядка формирования и ведения автоматизированных централизованных баз персональных данных о пассажирах и персонале (экипаже) транспортных средств, а также срока хранения и порядка предоставления содержащихся в них данных” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_477721/](https://www.consultant.ru/document/cons_doc_LAW_477721/) (Доступ: 21.08.2025).

<sup>103</sup> Медуза. “Мишустина предоставил ФСБ круглосуточный удаленный доступ к базам данных агрегаторов такси”. 07.07.2023 <https://meduza.io/news/2023/07/07/mishustin-predostavil-fsb-kruglosutochnyy-udalenny-dostup-k-bazam-danniyh-agregatorov-taksi> (Доступ: 21.08.2025).

<sup>104</sup> Алимова, Дина. “Депутаты Госдумы предлагают проводить видеосъемку поездок в такси”. Информационно-правовой портал ГАРАНТ.РУ (29.11.2024) <https://www.garant.ru/news/1770251/> (Доступ: 24.08.2025).

<sup>105</sup> Роскомсвобода. ““Яндекс.Заправки” и “Яндекс.Драйв” внесены в реестр по слежке за пользователями”. (02.02.2024) <https://roskomsvoboda.org/en/post/snova-yandex-v-slezhe/> (Доступ: 05.09.2025).

<sup>106</sup> Роскомсвобода. “Яндекс.Такси, Яндекс.Еда и другие сервисы компаний внесены в реестр по слежке”. (26.01.2022) <https://roskomsvoboda.org/en/post/snova-yandex-v-slezhe/> (Доступ: 05.09.2025).

<sup>107</sup> Скан, Оксана. “В Москве ввели верификацию для пользователей электросамокатов и велосипедов”. Информационно-правовой портал ГАРАНТ.РУ (10.02.2025) <https://www.garant.ru/article/1753211/> (Доступ: 05.09.2025).

“Паутина”. Некоторые дорожные камеры помимо стандартной видеосъемки и распознавание номеров могут распознавать лица водителей и пассажиров на переднем сиденье, а порой даже фиксировать пассажиров на задних сиденьях (хотя точность распознания лиц таких пассажиров пока остается под вопросом). В то же время неизвестно, ни точное число дорожных видеокамер (оценки колеблются от 30 до 50 тыс. единиц по данным на 2024 год), ни сколько из них подключены к системе распознавания лиц.

## 7. Постановка на учет / установка приложения по слежке

Весной 2025 года российские власти приняли закон, в котором установили, что в качестве “эксперимента” для нескольких категорий иностранных граждан требование миграционного учета, заменяется обязательной установкой приложения по отслеживанию геолокации<sup>108</sup>. С 1 сентября 2025 года требование по установке этого приложения, которое получило название “АМИНА”, распространяли на следующие категории иностранных граждан, которые приезжают в Москву и Московскую область в безвизовом порядке: 1) граждане Азербайджана, Украины, Таджикистана, Узбекистана, Молдовы и Грузии, прибывающие с целями осуществления трудовой деятельности по патенту, 2) граждане Кыргызстана, Казахстана и Армении, приехавшие с целью работы и освобожденные от получения разрешения на работу или патента, 3) приезжающие на срок свыше 90 дней и 4) тех, кто поменял цель приезда<sup>109</sup>. Из вышеперечисленных категорий граждан требования по установке приложения исключили граждан Беларуси, несовершеннолетних, сотрудников дипломатических/консульских учреждений. Новая программа слежки – еще один пример, демонстрирующий взаимосвязь слежки с помощью интернет и телефонии с отслеживанием физического перемещения и местопребывания. Очень вероятно, что власти планируют в будущем расширить новую программу слежки на иные категории иностранных граждан и другие регионы.

До нововведений 2025 года после въезда иностранный гражданин имел несколько дней (в зависимости от гражданства и целей въезда этот срок варьировался от семи до в редких случаях 90 дней) для постановки на миграционный учет, который был основным формальным инструментом по контролю за перемещением иностранных граждан<sup>110</sup>. Данные о миграционном учете поступали в ряд информационных систем, основными из которых были “Центральный банк данных по учету иностранных граждан и лиц без гражданства” (АС ЦБД УИГ)<sup>111</sup> и ГС МИР<sup>112</sup>. База данных позволяла сотрудникам полиции искать тех, кто либо не встал в положенный срок на миграционный учет, либо превысил сроки пребывания. В то же время в России была широко распространена продажа фиктивной постановки на

---

<sup>108</sup> Федеральный закон от 23.05.2025 N 121-ФЗ (ред. от 31.07.2025) “О внесении изменений в отдельные законодательные акты Российской Федерации и о проведении эксперимента по внедрению дополнительных механизмов учета иностранных граждан” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_505834/](https://www.consultant.ru/document/cons_doc_LAW_505834/) (Доступ: 20.08.2025).

<sup>109</sup> См. статья 5, пункт 3, там же.

<sup>110</sup> См. статью 4 здесь: Федеральный закон от 18.07.2006 N 109-ФЗ (ред. от 08.08.2024) “О миграционном учете иностранных граждан и лиц без гражданства в Российской Федерации” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_61569/](https://www.consultant.ru/document/cons_doc_LAW_61569/) (Доступ: 21.08.2025).

<sup>111</sup> Приказ МВД РФ, МИД РФ, ФСБ РФ, Министерства экономического развития и торговли РФ и Министерства информационных технологий и связи РФ от 10.03.2006 N 148/2562/98/62/25 “О ведении и использовании центрального банка данных по учету иностранных граждан и лиц без гражданства, временно пребывающих и временно или постоянно проживающих в Российской Федерации” <https://base.garant.ru/189312/> (Доступ: 21.08.2025).

<sup>112</sup> Постановление Правительства РФ от 06.08.2015 N 813 (ред. от 21.10.2024) “Об утверждении Положения о государственной системе миграционного и регистрационного учета, а также изготовления, оформления и контроля обращения документов, удостоверяющих личность” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_184040/](https://www.consultant.ru/document/cons_doc_LAW_184040/) (Доступ: 17.08.2025).

миграционный учет, проживание не по месту миграционного учета, частая смена адресов пребывания.

Программа по отслеживанию геолокации дополняет систему видеонаблюдения и отслеживание действий в Интернете, позволяя в реальном времени устанавливать точное фактическое место пребывания иностранного гражданина и выстраивать маршруты передвижений человека без необходимости наличия в этих местах видеокамер. Для предотвращения возможности смены СИМ-карт, приобретения обезличенных СИМ-карт, пользования различными мобильными телефонами российские власти приняли меры, которые были описаны выше, то есть обязали операторов мобильной связи прикреплять сим-карты к конкретному телефону, а затем эту сим-карту и телефон к конкретному иностранному гражданину.

Если иностранный гражданин начинает блокировать передачу данных геолокации, то через три дня его снимают с учета и он попадает в базу данных “контролируемых лиц”<sup>113</sup>, что влечет определенные последствиями, о которых мы расскажем чуть ниже. Примечательно, что, как и в случае с системой наблюдения, основным инспириатором новой программы стали власти Москвы, а курирование разработки приложения “АМИНА” занималось ГКУ “Информационный город”, подведомственное Департаменту информационных технологий Москвы.

## 8. Оформление миграционных документов / геномная регистрация

1 декабря 2024 года российские власти запустили еще один “эксперимент”, направленный на расширение и углубление слежки. Речь идет о “геномной регистрации” или “сборе биологических образцов”, установленных в рамках того же Постановление Правительства РФ от 7 ноября 2024 года<sup>114</sup>. Так, иностранный гражданин, который пересек перечисленные пограничные пункты в период проведения эксперимента (с 1 декабря 2024 года основные московские аэропорты и пункт пропуска в Оренбургской области, а с 30 июня 2025 года – все российские пропускные пункты) и который оформляет себе патент, разрешение на временное проживание или вид на жительство, а также подает документы на российское гражданство в Многофункциональном миграционном центре в Сахарово, обязывается сдать образцы ДНК и получить электронную карту иностранного гражданина.

Примечательно, в самом Постановлении Правительства РФ указывается, что иностранные граждане при обращении в Многофункциональный миграционный центр и осуществлении “обязательных процедур в сфере миграции” в то же время “проходят добровольную государственную геномную регистрацию” и “обязаны получить электронную карту иностранного гражданина”<sup>115</sup>. В чем “добровольность” геномной регистрации, которая относится к “обязательной процедуре”, документ не поясняет. И, очевидно, документ не устанавливает возможность получения, например, разрешения на временное проживание (РВП) или вида на жительство (ВиЖ), без “геномной регистрации”. Конечно, человек может развернуться и уйти, но это же касается и получения “электронной карты иностранного

---

<sup>113</sup> См. статью 5, пункт 21 здесь: Федеральный закон от 23.05.2025 N 121-ФЗ (ред. от 31.07.2025) “О внесении изменений в отдельные законодательные акты Российской Федерации и о проведении эксперимента по внедрению дополнительных механизмов учета иностранных граждан” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_505834/](https://www.consultant.ru/document/cons_doc_LAW_505834/) (Доступ: 20.08.2025).

<sup>114</sup> Постановление Правительства Российской Федерации от 07.11.2024 N 1510 “О проведении эксперимента по апробации правил и условий въезда в Российскую Федерацию и выезда из Российской Федерации иностранных граждан и лиц без гражданства” <https://www.garant.ru/products/ipo/prime/doc/410628090/> (Доступ: 17.08.2025)

<sup>115</sup> См. пункт 16, подпункт “б” там же.

гражданина”, относительно которой подчеркивается “обязательность”. Возможно, странные формулировки обусловлены попыткой авторов документа придать ему видимость наличия норм, которые защищают личные данные, свободу и приватность, при фактическом отсутствии этих норм. В документе отсутствует даже формальное пояснение, для чего российские власти собирают “биологические образцы” при том, что эта процедура требуется даже от детей (начиная с шести лет), недееспособных и пожилых людей.

Надо также отметить, что в Федеральном законе N 242-ФЗ от 03.12.2008 “О государственной геномной регистрации в Российской Федерации” обязательность сдачи образцов ДНК изначально относился лишь к заключенным и подследственным. Но российские власти решили расширить круг лиц и с 2025 года обязали сдавать образцы ДНК также тех, кто подвергнут административному аресту<sup>116</sup>. Иностранные граждане, оформляющие себе миграционные документы, к категории тех, кто обязан сдавать эти образцы, даже согласно новым поправкам, формально не относятся, хотя, как можно видеть, по факту российские власти их туда включили. Собранный “биологический материал” поступает в Федеральную базу данных геномной информации (ФБД ГeН), а также, согласно новым нормам, “лицо, уполномоченное на получение геномной информации, обеспечивает размещение геномной информации в информационных системах г. Москвы в форме электронной информационной карты”<sup>117</sup>.

Массовый сбор образцов ДНК несет в себе значительные риски и возможность злоупотреблений со стороны государства. Не случайно, что Европейский суд по правам человека признал принудительный сбор образцов ДНК с людей, которые не совершили тяжкого преступления, недопустимым вмешательством в частную жизнь (*Gaughan v. the United Kingdom*). В то же время российские власти не только расширили круг людей, у которых обязательно или под давлением собираются образцы ДНК, но и сделали доступ к геномной базе данных фактически неограниченным и безнадзорным для силовых ведомств<sup>118</sup>.

Имеет смысл упомянуть, что Россия - не единственная страна, которая занимается массовым сбором образцов ДНК. Так, В США уже несколько десятилетий действует программа, в рамках которых образцы ДНК берутся у осужденных и привлекаемых к уголовной ответственности. С 2020 года в США власти начали активно пополнять базу данных (Combined DNA Index System (CODIS) за счет мигрантов. В то же время следует выделить три принципиальных отличия программы США от российской программы: 1) образцы ДНК собираются лишь с тех мигрантов, которых задерживают и/или арестовывают власти в рамках уголовных и административных дел, 2) существует возможность отказа в случаях неправомерной попытки сбора этих данных, 3) как сама программа, так злоупотребления при ее выполнении подвергаются существенной критике и оспариваются правозащитными организациями и многими политиками<sup>119</sup>.

---

<sup>116</sup> См. статью 9 здесь: Федеральный закон N 242-ФЗ от 03.12.2008 “О государственной геномной регистрации в Российской Федерации” <https://base.garant.ru/12163758/> (Доступ: 21.08.2025).

<sup>117</sup> См. Пункты 18 и 20 здесь: Постановление Правительства Российской Федерации от 07.11.2024 N 1510 “О проведении эксперимента по апробации правил и условий въезда в Российскую Федерацию и выезда из Российской Федерации иностранных граждан и лиц без гражданства”. <https://www.garant.ru/products/ipo/prime/doc/410628090/> (Доступ: 17.08.2025).

<sup>118</sup> Lokhmurov, A. “Россия легализует массовый сбор ДНК-профилей граждан”. *Human Rights Watch* (09.02.2023) <https://www.hrw.org/ru/news/2023/02/09/russia-legalizes-massive-dna-collection-without-oversight> (Доступ: 21.08.2025).

<sup>119</sup> Georgetown Law. “Raiding the Genome: How the United States Government Is Abusing Its Immigration Powers to Amass DNA for Future Policing”. <https://www.law.georgetown.edu/privacy-technology-center/publications/raiding-the-genome/> (accessed August 21, 2025)

Программа по сбору образцов ДНК российскими властями скорее напоминает программу в Китае. Так, с 2017 года китайские власти качественно ускорили программу по принудительной геномной регистрации, запущенную еще в 2003 году. В начале эта программа (как и в России) распространялась на осужденных и привлекаемых к уголовной ответственности, но в 2013 году она была распространена на все население провинции Тибет, которая рассматривается китайскими властями как склонная к акциям протеста и сепаратизму. В 2016 году регистрация была распространена на другую “проблемную” и гораздо более крупную провинцию, а именно Синьцзян, где проживает большинство уйгуров. С 2017 года программа стала национальной и с тех пор были собраны сотни миллионов образцов ДНК (точное число неизвестно)<sup>120</sup>.

Помимо непосредственно расследований преступлений и легитимных случаев установления родства, сбор образцов ДНК открывает поле для возможных злоупотреблений и утечек данных. Среди возможных злоупотреблений следует упомянуть неавторизованное установление родственных связей, определение этнической принадлежности для установки целевой слежки и/или применения репрессий, исследование особенностей строения организма и предрасположенности к заболеваний в целях создания компромата, запугивания или целенаправленного заражения. Кроме того, есть косвенные данные, что собранные ДНК в Китае<sup>121</sup>, а, может быть, и в России<sup>122</sup>, помимо прочего используются для военных исследований. Последнее вызывает особую озабоченность в мире, поскольку, возможно, речь идет о так называемом “генетическом оружии” (genetic-based or biogenetic weapons), способном привести к ужасным и непредсказуемым последствиям.

## **9. Банковские операции, переводы, покупки и доставка / усиленное внимание**

Если иностранный гражданин желает открыть банковский счет, сделать перевод за границу, либо просто купить товар, используя кредитную карточку, то эти действия автоматически отслеживаются и обрабатываются, а в случае интереса со стороны силовых ведомств детально исследуются.

Российские власти уже не первый год активно используют банки для слежки и контроля, включая принудительные блокировки счетов и изымание средств. В 2020-х годах власти ввели множество новых норм, направленных на широкомасштабное включение банков в систему слежки, контроля и наказания. Следует впрочем упомянуть о пяти тенденциях, касающихся участия банков в системе слежки. Так, в последние годы российские власти, 1) расширили перечень ведомств, которые имеют доступ к банковской тайне и контролю за банковской системой (например, добавив в список налоговые органы, таможню и прокуроров), 2) внедрили ряд мер для легкого, быстрого и фактически неограниченного доступа широкого круга государственных ведомств практически к любой банковской информации, 3) ограничили банки в их участии в международном обмене информации и во многих случаях запретили им взаимодействие с иностранными финансовыми институтами, если отсутствует прямое государственное разрешение, 4) используют банки для сбора биометрических данных,

---

<sup>120</sup> Dirks, E.; Leibold, J. “Genomic Surveillance. Inside China's DNA dragnet”. ASPI (*Australian Strategic Policy Institute*), *International Cyber Policy Centre*. Report No. 34/2020. [https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-06/Genomic%20surveillance\\_1.pdf](https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-06/Genomic%20surveillance_1.pdf) (accessed August 21, 2025).

<sup>121</sup> Warrick, Joby and Cate Brown. “China's quest for human genetic data spurs fears of a DNA arms race”. *The Washington Post* (21.09.2023) <https://www.washingtonpost.com/world/interactive/2023/china-dna-sequencing-bgi-covid/> (accessed August 21, 2025).

<sup>122</sup> Petersen, Robert. “Fear and Loathing in Moscow. The Russian biological weapons program in 2022”. *Bulletin of the Atomic Scientists* (05.10.2022) <https://thebulletin.org/2022/10/the-russian-biological-weapons-program-in-2022/> (accessed August 22, 2025).

5) внедрили ряд механизмов по обязанию банков быстро и во внесудебном порядке блокировать счета, принудительно изымать средства и собирать с клиентов в интересах властей дополнительные данные<sup>123</sup>.

Помимо банков российские власти расширили слежку за пользователями интернет-площадок по продаже / обмене товаров и услуг (маркетплейсами и классифайдами). Так, согласно новым нормам, российские маркетплейсы (торговые площадки) и классифайды (доски объявлений) обязаны по запросу силовых ведомств (от ФСБ и МВД до Росгвардии и ФСО) быстро передавать данные о своих клиентах, что включает номер телефона, адрес электронной почты, информацию об реализованных покупках и услугах, а также специализированную техническую информацию о пользователях, среди которой IP-адрес, уникальный идентификатор пользователя на сайте (UID), идентификатор мобильного оборудования (IMEI), номер устройства в сети (MAC) и даже геолокацию устройства<sup>124</sup>.

Отслеживают российские власти также ряд сервисов по доставке. Так, крупнейшие российские сервисы, занимающиеся доставкой, а именно, Яндекс.Еда, Яндекс.Доставка, Яндекс.Лавка, с 2022 года находятся в реестре ОРИ, то есть силовые ведомства обязывают их делиться информацией о своих пользователях<sup>125</sup>.

Все эти меры касаются как российских, так и иностранных граждан. Что касается непосредственно последних, то тут российские власти приняли или намереваются принять ряд дополнительных норм, которые ставят эту категорию граждан даже под более пристальное наблюдение. Так, в конце марта 2025 года Росфинмониторинг предложил ограничить срок действия банковской карт для иностранных граждан одним годом, а также ввести дополнительные требования при открытии счета. В апреле 2025 года Генеральная прокуратура выступила с поддержкой идеи о дополнительном контроле банковских переводов, совершаемых мигрантами.

## **10. Попадание в реестр контролируемых лиц / ограничения и высылка из России**

Согласно нововведениям 2024 года, в случае, если алгоритмы миграционных информационных систем посчитают, что иностранный гражданин нарушил миграционные нормы, либо по каким-то причинам ФСБ или МВД аннулирует миграционные документы, то мигрант попадает в так называемый “реестр контролируемых лиц” (далее – РКЛ) и в отношении него активируется “режим высылки”<sup>126</sup>. РКЛ был запущен властями 5 февраля 2025 года, а уже в начале марта глава МВД объявил о том, что в нем числится 685 тыс. иностранных граждан<sup>127</sup>.

---

<sup>123</sup> Роскомсвобода. “Банкам запретили передавать данные о клиентах иностранным органам”. (20.04.2022) <https://roskomsvoboda.org/en/post/delitsya-banktaynoy-nelzya/> (Доступ: 21.08.2025).

<sup>124</sup> Роскомсвобода. “Силовики могут получить новые инструменты для слежки”. (20.05.2024) <https://roskomsvoboda.org/en/post/marketplace-data-access-rules-update/> (Доступ: 21.08.2025); Гаврилюк, Анастасия. “Шире круг: силовики получат данные о местоположении пользователей маркетплейсов”. *Forbes Russia* (19.06.2025).

<sup>125</sup> Роскомсвобода. “Яндекс.Такси, Яндекс.Еда и другие сервисы компаний внесены в реестр по слежке”. (26.01.2022) <https://roskomsvoboda.org/en/post/snova-yandex-v-slezhe/> (Доступ: 05.09.2025).

<sup>126</sup> См. статью 11 здесь: Федеральный закон от 08.08.2024 N 260-ФЗ “О внесении изменений в отдельные законодательные акты Российской Федерации” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_482512/](https://www.consultant.ru/document/cons_doc_LAW_482512/) (Доступ: 21.08.2025)

<sup>127</sup> Лебедева, О. “РФ включила в реестр контролируемых лиц 700 тыс. иностранцев”. Deutsche Welle (09.03.2025) <https://www.dw.com/ru/rf-vklucila-v-reestr-kontroliruemyh-lic-poeti-700-tysac-inostrancev/a-71871790> (Доступ: 21.09.2025).

Российские силовые ведомства с давних пор оперировали списками тех иностранных граждан, которые по их мнению нарушили миграционный режим. Списки составлялись на основании подсчетов по базам данных и системам, особо важными из которых, видимо, были Автоматизированная Система Центрального Банка Данных по Учету Иностранных Граждан и лиц без гражданства (АС ЦБД УИГ), а также автоматизированная информационная система “Криминал-И” (АИС Криминал-И). Однако, во-первых, эти списки не закреплялись отдельно законодательством, и, во-вторых, они были ориентировочными, поскольку попадание в эти списки, хотя и служило для ведомств, занимающихся миграцией, основанием для дополнительных проверок, но не вело к немедленным санкциям. Раньше, если оперативные сотрудники обнаруживали того или иного иностранного гражданина из списка, то они его проверяли, а в случае заключения сотрудников о подтверждении факта нарушения миграционного режима, мигранта задерживали и соответствующие судебные инстанции решали вопрос о наложении административного наказания и выдворения. Не так давно все это кардинально поменялось.

В 2024 году российские власти объявили о создании “реестра контролируемых лиц” и приняли Федеральный закон N 260-ФЗ от 08.08.2024 , вступивший в силу в начале 2025 года<sup>128</sup>. Этот реестр во многом объясняет, почему российские власти ускоренно внедряли новые технологии по слежке и столь настойчиво собирали многочисленные сведения с иностранных граждан до, во время и после их пересечения российских пограничных пунктов. Попадание в реестр контролируемых лиц влечет за собой ряд ограничительных мер, сильно осложняющих жизнь иностранного гражданина и которые напрямую связаны с системами слежки и контроля, описанными выше. Так, человеку, оказавшемуся в реестре, запрещено открывать банковский счет и делать банковские переводы, ему отказывают в праве зарегистрировать брак в ЗАГС, если он захочет переехать и встать на миграционный контроль, то в местном многофункциональном центре ему это не позволят сделать, если у него не будет специального разрешения от властей... и т.д. Координация этих мер, согласно установленным нормам, происходит на базе ЕСМЭВ. Это демонстрирует глубокий уровень централизации информационных систем и включение в него наряду с основными государственными ведомствами также негосударственных организаций.

Тот, кто попал в реестр контролируемых лиц, обязан оперативно и по первому требованию сообщать властям о своем местонахождении, объяснить, почему он не может выехать самостоятельно, являться в органы миграции. В случае если иностранный гражданин не выполняет какого-то из этого требования, оперативники миграционной службы будут его искать с задействованием системы слежки, описанной в нашем докладе. После обнаружения и задержания иностранному гражданину грозит немедленное помещение в депортационную тюрьму (центр временного содержания иностранных граждан или ЦВСИГ)<sup>129</sup>.

Попадание в РКЛ возможно по ряду оснований - от истекшего срока миграционных документов и задержки возвращение на круизные лайнеры до незаконного пересечения границы и осуждения по уголовной статье<sup>130</sup>. Важно отметить, что как включение, и так и исключение из РКЛ происходит “в автоматизированном режиме”<sup>131</sup>, даже формально не

<sup>128</sup> Федеральный закон от 08.08.2024 N 260-ФЗ “О внесении изменений в отдельные законодательные акты Российской Федерации” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_482512/](https://www.consultant.ru/document/cons_doc_LAW_482512/) (Доступ: 21.08.2025).

<sup>129</sup> Там же.

<sup>130</sup> Подробнее см., например, здесь: Кузнецова, Ирина. “Мигрантов поставят на учет: как ужесточат контроль за приезжими в России”. Информационно-правовой портал ГАРАНТ.РУ (12.08.2024) <https://www.garant.ru/article/1753211/> (Доступ: 21.08.2025).

<sup>131</sup> Постановление Правительства РФ от 26.12.2024 N 1899 “О реестре контролируемых лиц” (вместе с “Положением о реестре контролируемых лиц”)

подразумевая при этом санкции со стороны судебных инстанций. Все это нормативно закрепляет огромный простор для произвольных решений. Так, например, в перечень оснований для попадания реестра служит аннулирование документа, разрешающего пребывание (виза, РВП, ВнЖ). Аннулировать документы, согласно российскому законодательству, могут как в МВД, так и в ФСБ, при этом от них даже не требуется объяснять причины этого.

В отношении человека, попавшего в РКЛ, на нормативном уровне также закрепляется перечень допустимых способов слежки. Так, как следствие поправок в Федеральный закон “О правовом положении иностранных граждан в Российской Федерации”, появилась статья 31.1<sup>132</sup>, в котором полномочия сотрудников МВД качественным образом расширяются. Так, наибольшую полемику вызвало разрешение сотрудникам МВД проникать без какой-либо судебной санкции в любое помещение, в котором “пребывает (проживает) или фактически находится контролируемое лицо”. Далее, согласно поправкам, сотрудники МВД наделяются полномочиями по получению информации и документов “необходимых для осуществления контроля за контролируемым лицом”, в том числе тех, которые “составляют” банковскую, коммерческую и налоговую тайну, включая наличия и номера банковских счетов и движения по ним денежных средств. Обращает на себя внимание размытость формулировки, поскольку говорится не о информации в отношении контролируемого лица, а об информации “необходимой для осуществления контроля за контролируемым лицом”. Иными словами, сотрудники органов внутренних дел открыто наделяются полномочиями запроса информации о третьих лицах и организациях в рамках крайне неопределенной деятельности по “контролю за контролируемыми”.

Кроме того, в подпункте “7”, “8” и “9” статьи 31.3 того же закона указывается, что сотрудники МВД также имеют полномочия

“7) использовать технические средства (в том числе аппаратуру, осуществляющую аудио- и видеозапись, фотосъемку) и информацию, содержащуюся в государственных информационных системах и (или) базах данных государственных органов;

8) осуществлять наблюдение непосредственно или опосредованно, в том числе с использованием технических средств, за контролируемым лицом, совершаемыми контролируемым лицом действиями, а также за деятельностью физических и юридических лиц, оказывающих контролируемому лицу содействие в пребывании (проживании) на территории Российской Федерации, с учетом положений пунктов 15 и 16 статьи 31.1 настоящего Федерального закона;

9) использовать данные мобильных устройств и геолокации, платежных систем, работающих в автоматическом режиме специальных технических средств распознавания лиц”,<sup>133</sup>.

Бросается в глаза, насколько размыто и неопределенно сформулированы эти положения. Однако, если иметь в виду общую системы слежки, описанную выше, то становится ясно о чем идет речь. Очевидно, что, согласно этим параграфам, сотрудникам МВД позволяет знакомиться со сведениями, занесенными в базы данных, использовать систему видеокамер и

---

[https://www.consultant.ru/document/cons\\_doc\\_LAW\\_495039/24ff1b9f8b660e53e8f0c8b4d3a99d434ce594fd/](https://www.consultant.ru/document/cons_doc_LAW_495039/24ff1b9f8b660e53e8f0c8b4d3a99d434ce594fd/)  
(Доступ: 21.08.2025).

<sup>132</sup> Федеральный закон от 25.07.2002 N 115-ФЗ “О правовом положении иностранных граждан в Российской Федерации” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_37868/](https://www.consultant.ru/document/cons_doc_LAW_37868/) (Доступ: 21.08.2025).

<sup>133</sup> Там же.

программы по распознаванию лиц, искать человека по социальным сетям, проникать в мобильные устройства, читать переписку, отслеживать другую деятельность в интернете, смотреть банковские операции и денежные переводы, отслеживать геолокацию, осуществлять прослушки и т.п. Но, что примечательно, подобная слежка прямо санкционируется не только в отношении “контролируемого лица”, но и в отношении тех людей и организаций, которые оказывают “контролируемому лицу содействие в пребывании (проживании)”. При этом, судя по всему, интерпретация размытого смысла слова “содействие” остается на усмотрение самих сотрудников МВД.

Особо примечательно с РКЛ, что, используя изощренные новые технологии для слежки, российские власти в то же время демонстративно сняли с себя обязанность даже реального уведомления иностранного гражданина о попадании в этот реестр, хотя, учитывая объемы собираемых данных, во многих, а, вероятно, и в подавляющем большинстве случаев для них это не представляло бы никакого труда. Однако, российские власти цинично определили, что поскольку иностранный гражданин, попадая в этот реестр, может увидеть этот факт, сделав запрос на сайте МВД, то это уже означает “оповещение” иностранного гражданина об этом<sup>134</sup>.

---

<sup>134</sup> См. статью 11 по добавлению пункта 6 статьи 31.2 в Федеральный закон от 25 июля 2002 года N 115-ФЗ “О правовом положении иностранных граждан в Российской Федерации” здесь: Федеральный закон от 08.08.2024 N 260-ФЗ “О внесении изменений в отдельные законодательные акты Российской Федерации” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_482512/](https://www.consultant.ru/document/cons_doc_LAW_482512/) (Доступ: 21.08.2025).

## **Заключение**

Российские власти активно используют новые технологии наблюдения для создания системы тотальной слежки. Эта система состоит из четырех основных элементов: репрессивная политика, авторитарная структура власти, новые технологии и ограничительные нормативные акты. Все они отчетливы видны при исследовании системы слежки, направленной на иностранных граждан в России. В 2024 и 2025 годах многие нормативные нововведения российских властей касались именно иностранных граждан, включая ряд тех, которые вводили новые способы слежки. Так, помимо расширения и усиления общих способов слежки (системы видеонаблюдения, отслеживание действий в Интернете, мониторинг банковских операций и т.д.), которые распространяются на всех граждан, пребывающих на территориях, контролируемых российскими властями, в отношении обширных категорий иностранных граждан в 2024-2025 годах были дополнительно введены обязательный сбор образцов голоса, геномная регистрация и установка приложения по отслеживанию геолокации.

Как было показано в нашем докладе, российские власти еще до въезда иностранного гражданина стремятся сбить с него анкетные и биометрические данные, которые затем используются для слежки за ним и совершенствования системы слежки в целом. После въезда в Российскую Федерацию физические передвижения иностранного гражданина отслеживаются видеокамерами, системами учета и в ряде случаев также через приложение по определению геолокации, его действия в Интернет находятся под пристальным наблюдением, визит в банк, посещение государственных ведомств, обращение в МФЦ, перечисление денег, покупка через интернет, заказ такси, даже пользование услугами по доставке еды, то есть почти любое действие остается зафиксированным в памяти многочисленных баз данных, к которым российские силовые ведомства обычно имеют свободный доступ. В случае, если системы миграционного контроля заключают, что иностранный гражданин нарушил миграционные правила, то в отношении него автоматически активируется “режим высылки”, мигрант оказывается еще более ограниченным в свободе передвижения, пользование банковским счетом, возможностью совершать покупки и в ряде других операций, а его действия начинают еще более внимательно отслеживаться.

Российские власти разрабатывают и используют новые технологии наблюдения для все расширяющейся слежки за иностранными гражданами, не обращая при этом внимания на защиту их прав. Нормативные акты, которые расширяют имеющиеся системы слежки и вводят новые, носят противоречивый и преимущественно антиправовой характер. Силовые ведомства, которые и до нововведений 2020-х годов обладали излишне широкими полномочиями по слежке, в последние годы получили доступ фактически к любому аспекту жизни иностранного гражданина, находящегося на территориях, контролируемых российскими властями. В то же время многие системы и технологии слежки действуют в общем режиме, то есть без различия на иностранных и российских граждан. Что касается слежки, направленной именно на иностранных граждан, то нельзя исключить, что власти тестируют на иностранных гражданах новые способы слежки с целью их возможного дальнейшего использования также на российских гражданах.

## **Использованная литература и нормативные акты**

### *Литература*

- Александров, А. “В России начали широко рекламировать мессенджер Max. В чем его опасность и способен ли он стать аналогом китайского WeChat?” *Настоящее время* (14.07.2025) <https://www.currenttime.tv/a/v-rossii-nachali-shiroko-reklamirovat-messendzher-max-v-chem-ego-opasnost-i-sposoben-li-on-stat-analogom-kitayskogo-wechat-33472932.html> Доступ: 21.10.2025.
- Алимова, Дина. “Депутаты Госдумы предлагают проводить видеосъемку поездок в такси”. *Информационно-правовой портал ГАРАНТ.РУ* (29.11.2024) <https://www.garant.ru/news/1770251/> (Доступ: 24.08.2025).
- Бородихин, А. “Корона доказательств. Как устроено ‘санитарное дело’”. *Медиазона* (07.07.2021) <https://zona.media/article/2021/07/07/korona-236> (Доступ: 15.08.2025).
- Гаврилюк, Анастасия. “Контрольная работа: городские камеры научат слышать звуки и распознавать силуэты”. *Forbes Russia* (13.02.2024).
- Гаврилюк, Анастасия. “Сдугая камера: Минцифры намерено создать платформу видеонаблюдения за 2 млрд рублей”. *Forbes Russia* (13.01.2025).
- Гаврилюк, Анастасия. “Шире круг: силовики получат данные о местоположении пользователей маркетплейсов”. *Forbes Russia* (19.06.2025).
- Глухова, Н.; Борисенко, Л. “Где и как в России отключают интернет”. *Новая газета Европа* (08.07.2025) <https://novayagazeta.eu/articles/2025/07/08/gde-i-kak-v-rossii-otkliuchaiut-internet> (Доступ: 20.08.2025).
- Дик, С.; Тихомирова, О. “Наказание за поиск в Сети. Какие штрафы грозят россиянам”. *Deutsche Welle* (23.07.2025) <https://www.dw.com/ru/nakazanie-za-poisk-v-internete-kakie-strafy-grozat-rossianam/a-73388354> (Доступ: 19.08.2025).
- Дмитриев Д., Яппарова Л. “Власти задумали сделать единую систему видеонаблюдения (как в Москве, только по всей стране). Из утечки документов администрации президента мы узнали, кто ее разрабатывает”. *Медуза* (29.02.2024) <https://meduza.io/feature/2024/02/29/vlasti-zadumali-sdelat-edinuyu-sistemu-videoonablyudeniya-kak-v-moskve-tolko-po-vseye-strane-iz-utechki-dokumentov-administratsii-prezidenta-my-uznali-kto-ee-razrabatyvaet> (Доступ: 15.08.2025).
- Доклад Специального докладчика ООН по вопросу о поощрении и защите права на свободу мнений и их свободное выражение. “Слежение и права человека”. *Совет по правам человека*. Сорок первая сессия 24 июня — 12 июля 2019 года. <https://digitallibrary.un.org/record/3814512?ln=en&v=pdf> (Доступ: 17.08.2025).
- Доклад Управления Верховного комиссара ООН по правам человека. “Права человека и новые и появляющиеся цифровые технологии”. *Совет по правам человека*. Пятьдесят шестая сессия 18 июня — 12 июля 2024 года. <https://docs.un.org/ru/A/HRC/56/45> (Доступ: 09.08.2025).
- Доклад Управления Верховного комиссара Организации Объединенных Наций по правам человека. “Право на неприкосновенность частной жизни в цифровую эпоху”. *Совет по правам человека*. Пятьдесят первая сессия 12 сентября — 7 октября 2022 года <https://docs.un.org/ru/A/HRC/51/17> (Доступ: 08.08.2025).
- Дульнева, М. “‘Тинькофф’ и Сбербанк теперь передают биометрические данные клиентов властям. Чем опасно хранение таких данных в государственной системе — и как запретить их использовать?” *Медуза* (12.10.2023) <https://meduza.io/cards/tinkoff-i-sberbank-teper-peredayut-biometricheskie-dannye-klientov-vlastyam-chem-opasno-hranenie-takih-dannyh-v-gosudarstvennoy-sisteme-i-kak-zapretit-ih-ispolzovat> (Доступ: 20.08.2025).
- Издание “Бумага”. “Как оппозиционеров задерживают с помощью распознавания лиц. Рассказываем о московской системе ‘Сфера’ и ее аналоге в Петербурге.” 15.06.2022 <https://paperpaper.io/kak-oppozionerov-zaderzhivayut-s-pom/> (Доступ: 21.08.2025).

- Захаров, Андрей. ““Умный город’ или ‘Старший брат’? Как мэрия научилась знать о москвичах всё”. *BBC News Русская служба* (10.04.2020) <https://www.bbc.com/russian/features-52219260> (Доступ: 05.08.2025).
- Захаров, Андрей. “Злость, страх и силуэты. Мэрия Москвы раскрыла, какие алгоритмы распознают людей по лицам.” *BBC News Русская служба* (25.08.2022) <https://www.bbc.com/russian/features-62658404> (Доступ: 18.08.2025).
- Кагермазов, С.; Попова, А. “Не самый надежный мессенджер? Основные вопросы о Telegram.” *BBC News Русская служба* (11.06.2025) <https://www.bbc.com/russian/articles/c0lndgzwwn1o> (Доступ: 19.08.2025).
- Ковачич, Леонид. “Сделано не в Китае: как устроена система видеонаблюдения Москвы”. *Московский центр Карнеги* (15.08.2020) <https://carnegie.ru/2020/08/05/ru-pub-82419> (Доступ: 15.08.2025).
- Комитет по правам человека ООН. “Заключительные замечания по восьмому периодическому докладу Российской Федерации” (октябрь-ноябрь 2022) <https://docs.un.org/ru/CCPR/C/RUS/CO/8> (Доступ: 15.08.2025).
- Коржова, Дарья. “Самозапреты и отключения: власти запланировали меры по защите граждан в интернете”, *Forbes Russia* (21.08.2025).
- Кузнецова, Ирина. “Мигрантов поставят на учет: как ужесточат контроль за приезжими в России”. *Информационно-правовой портал ГАРАНТ.РУ* (12.08.2024) <https://www.garant.ru/article/1753211/> (Доступ: 21.08.2025).
- Лебедева, О. “РФ включила в реестр контролируемых лиц 700 тыс. иностранцев”. *Deutsche Welle* (09.03.2025) <https://www.dw.com/ru/rf-vklucila-v-reestr-kontroliruemyh-lic-posti-700-tysac-inostrancev/a-71871790> (Доступ: 21.09.2025).
- Легалов, Евгений. “Небольшой брат. Как видеокамеры стали инструментом репрессий”. *Радио Свобода* (07.05.2024) <https://www.svoboda.org/a/neboljshoy-brat-kak-videoekamery-stali-instrumentom-repressiy/32932369.html> (Доступ: 15.08.2025).
- Литвин, В. “Достали из бани”. *Новая Газета Европа* (15.08.2024) <https://novayagazeta.eu/articles/2024/08/15/dostali-iz-bani> (Доступ: 19.08.2025)
- Медуза. “Мишустин предоставил ФСБ круглосуточный удаленный доступ к базам данных агрегаторов такси”. 07.07.2023 <https://meduza.io/news/2023/07/07/mishustin-predostavil-fsb-kruglosutochnyy-udalenny-dostup-k-bazam-danniyh-agregatorov-taksi> (Доступ: 21.08.2025).
- Медуза. “VK перешел под контроль Газпромбанка и «Согаза» друга Путина Юрия Ковалчука. Гендиректором VK станет сын Сергея Кириенко”. (03.12.2021) [https://meduza.io/feature/2021/12/03/vk-pereshel-pod-kontrol-gazprombanka-i-sogaza-druga-putina-yuriya-kovalchuka-gendirektorom-vk-stanet-syn-sergeya-kirienko](https://meduza.io/feature/2021/12/03/vk-pereshel-pod-kontrol-gazprombanka-i-sogaza-drugaputina-yuriya-kovalchuka-gendirektorom-vk-stanet-syn-sergeya-kirienko) (Доступ: 23.08.2025).
- Медуза. “Мессенджер Max начнут предустанавливать на все смартфоны в России с 1 сентября”. 21.08.2025 <https://meduza.io/news/2025/08/21/messendzher-max-stanut-predustanavlivat-na-vse-smartfony-v-rossii-s-1-sentyabrya> (Доступ: 21.08.2025).
- Мемориал: Центр Защиты Прав Человека. “Задержания мигрантов в Москве: комментарии юристов”. (19.06.2024) <https://memorialcenter.org/ru/news/zaderzhaniya-migrantov-v-moskve-komentarii-yuristov-1> (Доступ: 19.08.2025).
- ОВД-Инфо. “Как власти используют камеры и распознавание лиц против протестующих,” 17.02.2022, <https://reports.ovd.info/kak-vlasti-ispolzuyut-kamery-i-raspoznavanie-lic-protiv-protestuyushchih> (доступ 12 августа 2025 года).
- ОВД-Инфо и Роскосвобода. “Права человека и новые технологии в России”. 06.03.2023, <https://reports.ovd.info/prava-cheloveka-i-novye-tehnologii-v-rossii> (доступ 8 августа 2025 года).
- Онейда, Тесса. “Россия и Беларусь подписали соглашение: будут обмениваться данными о пересечении границы.” *Belsat* (04.04.2025) <https://ru.belsat.eu/85988964/rossiya-i-belarus-obmenivayutsya-dannymi-o-pereschenii-granicy> (Доступ: 02.10.2025).

Позычанюк, В.; Мироненко, П. “ФСБ потребовала от интернет-сервисов онлайн-доступ к данным и переписке пользователей”. *The Bell* (11.02.2020) <https://thebell.io/fsb-potrebovala-ot-internet-servisov-onlajn-dostup-k-dannym-i-perepiske-polzovatelei> (Доступ: 19.08.2025).

Радио Свобода. Idel.Реалии. “Камеры в Санкт-Петербурге начнут распознавать ‘этническую идентичность’, чтобы следить за мигрантами”. (20.02.2025) <https://www.idelreal.org/a/kamery-v-peterburge-nastroyat-na-raspoznavanie-etnosa/33321484.html> (Доступ: 19.08.2025).

Редакция “Вёрстка”. “Власти ограничили доступ к рекордному числу сайтов в 2024 году — более чем к 417 тысячам”. *Вёрстка* (28.01.2025) <https://verstka.media/vlasti-ogranichili-dostup-k-rekordnomu-chislu-saitov-v-2024-godu-bolee-chem-k-417k-news> (Доступ: 20.08.2025).

Роскомсвобода. “На столичную систему видеонаблюдения потратят порядка 28,5 млрд рублей”. (10.11.2020) <https://roskomsvoboda.org/ru/66160/> (Доступ: 22.09.2025).

Роскомсвобода. “В Москве хотят подключить камеры ТЦ к городской системе видеонаблюдения”. (20.10.2021) <https://roskomsvoboda.org/en/post/kamery-maski-kontrol/> (Доступ: 18.08.2025).

Роскомсвобода. “Яндекс.Такси, Яндекс.Еда и другие сервисы компании внесены в реестр по слежке”. (26.01.2022) <https://roskomsvoboda.org/en/post/snova-yandex-v-slezhe/> (Доступ: 05.09.2025).

Роскомсвобода. “Банкам запретили передавать данные о клиентах иностранным органам”. (20.04.2022) <https://roskomsvoboda.org/en/post/delitsya-banktaynoy-nelzya/> (Доступ: 21.08.2025).

Роскомсвобода. “Столичная мэрия заглянет в ночные клубы... через камеры видеонаблюдения”. (04.05.2022) <https://roskomsvoboda.org/en/post/podglyadet-zanochikami/> (Доступ: 18.08.2025).

Роскомсвобода. “‘Яндекс.Заправки’ и ‘Яндекс.Драйв’ внесены в реестр по слежке за пользователями”. (02.02.2024) <https://roskomsvoboda.org/en/post/snova-yandex-v-slezhe/> (Доступ: 05.09.2025).

Роскомсвобода. “Каждая третья камера видеонаблюдения подключена к системам распознавания”. (12.03.2024) <https://roskomsvoboda.org/en/post/kamery-bezgorod-ai/> (Доступ: 18.08.2025).

Роскомсвобода. “Подключение вообще всех камер к системам Москвы – это кошмар и ужас”. (20.05.2024) <https://roskomsvoboda.org/ru/post/video-camera-coffee-shop/> (Доступ: 18.08.2025).

Роскомсвобода. “Силовики могут получить новые инструменты для слежки”. (20.05.2024) <https://roskomsvoboda.org/en/post/marketplace-data-access-rules-update/> (Доступ: 21.08.2025).

Роскомсвобода. “Петербургские видеокамеры научили распознавать этническую принадлежность”. (25.08.2025) <https://roskomsvoboda.org/ru/post/ethnicity-detection-cctv-russia-policy/> (Доступ: 26.09.2025).

Рофе, Ж. “Иностранцев в РФ, не сдавших биометрию, лишат сим-карт”. *Deutsche Welle* (01.07.2025) <https://www.dw.com/ru/inostrancev-v-rossii-ne-sdavsih-biometriu-lisatsimkart/a-73109351> (Доступ: 20.08.2025).

Скан, Оксана. “В Москве ввели верификацию для пользователей электросамокатов и велосипедов.” *Информационно-правовой портал ГАРАНТ.РУ* (10.02.2025) <https://www.garant.ru/article/1753211/> (Доступ: 05.09.2025).

Солдатов Андрей и Ирина Бороган. *Новое дворянство: Очерки истории ФСБ*. Москва. Альпина Бизнес Букс, 2012.

Солдатов Андрей и Ирина Бороган. *Битва за Рунет: Как власть манипулирует информацией и следит за каждым из нас*. Москва, Альпина Паблишер, 2017.

- Шестаков, К. “В РФ проводят учения по отключению от зарубежного интернета”. *Deutsche Welle* (06.12.2024) <https://www.dw.com/ru/v-rossii-provoda-ucenia-po-otkluceniu-ot-zarubeznogo-interneta/a-70989516> (Доступ: 20.08.2025).
- Ширер, Дэвид. Р. *Сталинский военный социализм. Репрессии и общественный порядок в Советском Союзе, 1924-1953 гг.* Москва, РОССПЭН, 2014.
- Access, EFF, Privacy International, et. al. “Международные принципы по соблюдению прав человека при использовании слежки в коммуникациях”. <https://necessaryandproportionate.org/ru/%D0%BF%D1%80%D0%B8%D0%BD%D1%86%D0%B8%D0%BF%D1%8B/> (Доступ: 19.08.2025).
- Applebaum, A. *Autocracy, INC. The Dictators Who Want to Run the World*. New York, Doubleday, 2024.
- Dietrich, P. “The Key Player in Russia’s Cybersphere. What the West Needs to Know about VK Company”. *German Council on Foreign Relations* (20.09.2023) <https://dgap.org/en/research/publications/key-player-russias-cybersphere> (accessed August 19, 2025).
- Dirks, E.; Leibold, J. “Genomic Surveillance. Inside China's DNA dragnet”. ASPI (Australian Strategic Policy Institute), *International Cyber Policy Centre*. Report No. 34/2020. [https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-06/Genomic%20surveillance\\_1.pdf](https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-06/Genomic%20surveillance_1.pdf) (accessed August 21, 2025).
- Epifanova, Alena. “Deciphering Russia’s ‘Sovereign Internet Law.’ Tightening Control and Accelerating the Splinternet”. *German Council on Foreign Relations*. January 2020. [https://dgap.org/sites/default/files/article\\_pdfs/dgap-analyse\\_2-2020\\_epifanova\\_0.pdf](https://dgap.org/sites/default/files/article_pdfs/dgap-analyse_2-2020_epifanova_0.pdf) (accessed August 14, 2025).
- Feldstein, Steven. *The Rise of Digital Repression. How Technology Is Reshaping Power, Politics, and Resistance*. Oxford, Oxford University Press, 2021.
- Freedom House. “Freedom On the Net 2024”. October 2024, <https://freedomhouse.org/sites/default/files/2024-10/FREEDOM-ON-THE-NET-2024-DIGITAL-BOOKLET.pdf> (accessed October 3, 2025).
- Georgetown Law. “Raiding the Genome: How the United States Government Is Abusing Its Immigration Powers to Amass DNA for Future Policing”. <https://www.law.georgetown.edu/privacy-technology-center/publications/raiding-the-genome/> (accessed August 21, 2025).
- Gohdes, A.R. *Repression in the Digital Age. Surveillance, Censorship, and the Dynamics of State Violence*. Oxford, Oxford University Press, 2024.
- Human Rights Watch. “Living in Fear and Humiliation. Rising Xenophobic Harassment and Violence towards Central Asian Migrants in Russia”. March, 2025, [https://www.hrw.org/sites/default/files/media\\_2025/04/russia0325web.pdf](https://www.hrw.org/sites/default/files/media_2025/04/russia0325web.pdf) (accessed August 22, 2025).
- Human Rights Watch. “Disrupted, Throttled, and Blocked State Censorship, Control, and Increasing Isolation of Internet Users in Russia”. July, 2025, [https://www.hrw.org/sites/default/files/media\\_2025/07/russia0725%20web.pdf](https://www.hrw.org/sites/default/files/media_2025/07/russia0725%20web.pdf) (accessed August 8, 2025).
- Insikt Group. “Tracking Deployment of Russian Surveillance Technologies in Central Asia and Latin America”. (07.01.2025) <https://go.recordedfuture.com/hubfs/reports/ta-ru-2025-0107.pdf> (accessed August 20, 2025).
- International Partnership for Human Rights (IPHR) and Global Diligence LLP. “Russia's Digital Authoritarianism: the Kremlin's Toolkit,” September, 2023 <https://iphronline.org/articles/russias-digital-authoritarianism-the-kremlins-toolkit/> (accessed August 12, 2025).
- Kislov, Daniil and Ernest Zhanaev. “Russia: Xenophobia and vulnerability of migrants from Central Asia”. *The Foreign Policy Centre* (04.12.2017) <https://fpc.org.uk/russia-xenophobia-vulnerability-migrants-central-asia/> (accessed August 22, 2025).

- Kócsi, B.; Finn, B. "Investigating WeChat: An introduction to social apps WeChat and Weixin". *Reporters Without Borders* (12.08.2024) <https://safety.rsf.org/investigating-wechat-an-introduction-to-social-apps-wechat-and-weixin/> (accessed August 20, 2025).
- Krolik, A.; Mozur, P.; Satariano, A. "Cracking Down on Dissent, Russia Seeds a Surveillance Supply Chain". *The New York Times* (03.07.2023) <https://www.nytimes.com/2023/07/03/technology/russia-ukraine-surveillance-tech.html> (accessed August 19, 2025).
- Marx, Gary. *Windows into the Soul. Surveillance and Society in an Age of High Technology*. The University of Chicago Press, 2016.
- Lokhmutov, A. "Россия легализует массовый сбор ДНК-профилей граждан". *Human Rights Watch* (09.02.2023) <https://www.hrw.org/ru/news/2023/02/09/russia-legalizes-massive-dna-collection-without-oversight> (Доступ: 21.08.2025).
- Lyon, David. *Surveillance*. Oxford, Oxford University Press, 2024.
- Mahon, Anastassiya and Scott Walker. "Russia's Digital Repression Landscape: Unraveling the Kremlin's Digital Repression Tactics". *Journal of Illiberalism Studies*. 2024. Vol. 4. No. 3. P. 29-50.
- Pearson, James. S. "Defining Digital Authoritarianism". *Philosophy & Technology*. 2024. Vol. 37. No. 73. <https://link.springer.com/article/10.1007/s13347-024-00754-8#Fn2> (accessed October 4, 2025).
- Pei, M. *The Sentinel State. Surveillance and the Survival of Dictatorship in China*. Cambridge, Harvard University Press, 2024.
- Petersen, J.K. *Introduction to Surveillance Studies*. Boca Raton, Taylor & Francis Group, 2013.
- Petersen, Robert. "Fear and Loathing in Moscow. The Russian biological weapons program in 2022". *Bulletin of the Atomic Scientists* (05.10.2022) <https://thebulletin.org/2022/10/the-russian-biological-weapons-program-in-2022/> (accessed August 22, 2025).
- Reporters Without Borders. "Taking Control? Internet Censorship and Surveillance in Russia". 2019. [https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Downloads/Berichte/2019/russiareport\\_web\\_updated.pdf](https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Downloads/Berichte/2019/russiareport_web_updated.pdf) (accessed August 18, 2025).
- Shearer, David R. *Stalin's Socialism. Repression and Social Order in the Soviet Union, 1924-1953*. New Haven and London, Yale University Press, 2009.
- Soldatov, A., Borogan, I. "Digital Surveillance and the Impact on Journalism in Russia". *Friedrich Naumann Foundation for Freedom*, (2020) <https://shop.freihheit.org/#!/Publikation/943> (accessed August 18, 2025).
- Soldatov, A., Borogan, I. "The New Iron Curtain". *The Center for European Policy Analysis* (CEPA). June 7, 2022 <https://cepa.org/comprehensive-reports/the-new-iron-curtain-2/> (accessed August 14, 2025).
- The Insider. "VK представила 'российский WeChat': приложение получает доступ к микрофону, камере и передает данные властям. Главное о мессенджере". <https://theins.ru/news/281890> (05.06.2025) (Доступ: 20.08.2025).
- The Moscow Times. "'Отказаться нельзя'. Гостиницы Москвы обязали подключиться с государственной системе видеослежки за гражданами". (19.10.2022) <https://www.moscowtimes.ru/2022/10/19/otkazatsya-nelzya-gostintsi-moskvi-obyazali-podklyuchitsya-s-gosudarstvennoi-sisteme-videoslezhki-za-grazhdanami-a25487> (Доступ: 18.08.2025).
- The Moscow Times. "Три четверти российских регионов внедрили системы слежки за гражданами". (24.10.2023) <https://www.moscowtimes.ru/2023/10/24/tri-chetverti-rossiiskih-regionov-vnedrili-sistemi-slezhki-za-grazhdanami-a111011> (Доступ: 18.08.2025).
- Ünver, A. *Artificial intelligence (AI) and human rights: Using AI as a weapon of repression and its impact on human rights*. Brussels, European Union, 2024 [https://www.europarl.europa.eu/thinktank/en/document/EXPO\\_IDA\(2024\)754450](https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2024)754450) (accessed August 19, 2025).

Warrick, Joby and Cate Brown. "China's quest for human genetic data spurs fears of a DNA arms race". The Washington Post (21.09.2023) <https://safety.rsf.org/investigating-wechat-and-introduction-to-social-apps-wechat-and-weixin/> (accessed August 21, 2025).

Weller, Toni. "The historical ubiquity of surveillance". In edited by Andreas Marklund & Laura Skouwig, *Histories of Surveillance from Antiquity to the Digital Era*. London and New York, Routledge, 2022.

Zuckerman, Fredric S. *The Tsarist Secret Police in Russian Society, 1880-1917*. New York, New York University Press, 1996.

### *Нормативные акты*

- Закон РФ “О Государственной границе Российской Федерации” от 01.04.1993 N 4730-1 [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_3140/](https://www.consultant.ru/document/cons_doc_LAW_3140/) (Доступ: 18.08.2025).
- Письмо Минцифры России от 17.06.2025 N ОК-П24-58177 “О разъяснении правил, вводимых на территории Российской Федерации постановлением Правительства РФ от 07.11.2024 N 1510” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_509343/](https://www.consultant.ru/document/cons_doc_LAW_509343/) (Доступ: 18.08.2025).
- Постановление Правительства Москвы от 17.03.2021 N 328-ПП “О государственной автоматизированной информационной системе “Сфера”” <https://base.garant.ru/400484831/> (Доступ: 23.08.2025).
- Постановление Правительства Москвы от 21.01.2025 N 47-ПП “О внесении изменений в постановления Правительства Москвы от 16 июня 2011 г. N 272-ПП и от 19 мая 2015 г. N 299-ПП” <https://www.consultant.ru/law/review/209259861.html> (Доступ: 18.08.2025).
- Постановление Правительства РФ от 08.09.2010 N 697 (ред. от 28.11.2024) “О единой системе межведомственного электронного взаимодействия” (вместе с “Положением о единой системе межведомственного электронного взаимодействия”) [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_104665/59a1ee33e6096f0bf3fd23d27\\_eeb41a502ed129e/#dst30](https://www.consultant.ru/document/cons_doc_LAW_104665/59a1ee33e6096f0bf3fd23d27_eeb41a502ed129e/#dst30) (Доступ: 18.08.2025).
- Постановление Правительства РФ от 31.07.2014 N 743 “Об утверждении Правил взаимодействия организаторов распространения информации в информационно-телекоммуникационной сети ‘Интернет’ с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации” <https://base.garant.ru/70709018/> (Доступ: 19.08.2025).
- Постановление Правительства РФ от 06.08.2015 N 813 (ред. от 21.10.2024) “Об утверждении Положения о государственной системе миграционного и регистрационного учета, а также изготовления, оформления и контроля обращения документов, удостоверяющих личность” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_184040/](https://www.consultant.ru/document/cons_doc_LAW_184040/) (Доступ: 17.08.2025).
- Постановление Правительства РФ от 26.09.2016 N 969 “Об утверждении требований к функциональным свойствам технических средств обеспечения транспортной безопасности и Правил обязательной сертификации технических средств обеспечения транспортной безопасности” <https://base.garant.ru/71500596/> (Доступ: 24.08.2025).
- Постановление Правительства РФ от 07.11.2020 N 1793 “О порядке оформления единых электронных виз и признании утратившими силу некоторых актов Правительства Российской Федерации” (вместе с “Положением о порядке оформления единых электронных виз”). [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_367444/47e1f3ca06b495c2673ba8e2\\_e466a0fea84c4f8/](https://www.consultant.ru/document/cons_doc_LAW_367444/47e1f3ca06b495c2673ba8e2_e466a0fea84c4f8/) (Доступ: 17.08.2025).
- Постановление Правительства РФ от 29.08.2024 N 1180 “О внесении изменения в постановление Правительства Российской Федерации от 6 августа 2015 г. N 813” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_484735/](https://www.consultant.ru/document/cons_doc_LAW_484735/) (Доступ: 08.10.2025).

- Постановление Правительства Российской Федерации от 07.11.2024 N 1510 “О проведении эксперимента по апробации правил и условий въезда в Российскую Федерацию и выезда из Российской Федерации иностранных граждан и лиц без гражданства” <https://www.garant.ru/products/ipo/prime/doc/410628090/> (Доступ: 17.08.2025).
- Постановление Правительства РФ от 26.12.2024 N 1899 “О реестре контролируемых лиц” (вместе с “Положением о реестре контролируемых лиц”) [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_495039/24ff1b9f8b660e53e8f0c8b4d3a99d434ce594fd/](https://www.consultant.ru/document/cons_doc_LAW_495039/24ff1b9f8b660e53e8f0c8b4d3a99d434ce594fd/) (Доступ: 21.08.2025).
- Постановление Правительства РФ от 13.02.2025 N 156 “О внесении изменений в постановление Правительства Российской Федерации от 27 мая 2021 г. N 810” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_499251/](https://www.consultant.ru/document/cons_doc_LAW_499251/) (Доступ: 24.08.2025).
- Постановления Совета Министров Республики Беларусь от 31.03.2025 № 192 “Об информационной системе обмена сведениями”.
- Приказ МВД РФ, МИД РФ, ФСБ РФ, Министерства экономического развития и торговли РФ и Министерства информационных технологий и связи РФ от 10.03.2006 N 148/2562/98/62/25 “О ведении и использовании центрального банка данных по учету иностранных граждан и лиц без гражданства, временно пребывающих и временно или постоянно проживающих в Российской Федерации” <https://base.garant.ru/189312/> (Доступ: 21.08.2025).
- Приказ МИД России от 31.05.2017 N 9175 “Об утверждении Порядка организации деятельности Министерства иностранных дел Российской Федерации по оформлению, выдаче, продлению срока действия визы, восстановлению либо аннулированию визы, а также порядка учета и хранения бланков виз” <https://base.garant.ru/71709404/> (Доступ: 17.08.2025).
- Приказ МИД России от 14.12.2020 N 22683 “Об утверждении состава сведений, которые указываются иностранным гражданином в заявлении об оформлении единой электронной визы, а также форм уведомлений об оформлении и об отказе в оформлении единой электронной визы.” <https://base.garant.ru/400103460/> (Доступ: 21.08.2025).
- Приказ Минтранса России от 02.05.2024 N 162 “Об утверждении порядка формирования и ведения автоматизированных централизованных баз персональных данных о пассажирах и персонале (экипаже) транспортных средств, а также срока хранения и порядка предоставления содержащихся в них данных” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_477721/](https://www.consultant.ru/document/cons_doc_LAW_477721/) (Доступ: 21.08.2025).
- Распоряжение Правительства РФ от 03.12.2014 N 2446-р “Об утверждении Концепции построения и развития аппаратно-программного комплекса ‘Безопасный город’” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_172077/](https://www.consultant.ru/document/cons_doc_LAW_172077/) (Доступ: 15.08.2025).
- Указ Президента РФ от 31.10.2018 N 622 “О Концепции государственной миграционной политики Российской Федерации на 2019 - 2025 годы” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_310139/74e338ae02b148ec31de4bc38f486b8b045d3a1e/](https://www.consultant.ru/document/cons_doc_LAW_310139/74e338ae02b148ec31de4bc38f486b8b045d3a1e/) (Доступ: 15.08.2025).
- Указ Президента Российской Федерации от 09.07.2025 N 467 “О государственном информационном ресурсе ‘Цифровой профиль иностранного гражданина’” <https://www.garant.ru/products/ipo/prime/doc/412204934/> (Доступ: 18.08.2025).
- Указ Президента РФ от 15..10.2025 N 738 “О Концепции государственной миграционной политики Российской Федерации на 2026 - 2030 годы” <https://www.garant.ru/hotlaw/federal/1887540/> (Доступ: 17.10.2025).
- Федеральный закон от 25.07.2002 N 115-ФЗ “О правовом положении иностранных граждан в Российской Федерации” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_37868/](https://www.consultant.ru/document/cons_doc_LAW_37868/) (Доступ: 21.08.2025).

- Федеральный закон от 18.07.2006 N 109-ФЗ (ред. от 08.08.2024) “О миграционном учете иностранных граждан и лиц без гражданства в Российской Федерации” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_61569/](https://www.consultant.ru/document/cons_doc_LAW_61569/) (Доступ: 21.08.2025).
- Федеральный закон от 03.12.2008 N 242-ФЗ “О государственной геномной регистрации в Российской Федерации” <https://base.garant.ru/12163758/> (Доступ: 21.08.2025).
- Федеральный закон от 05.05.2014 N 97-ФЗ “О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации” и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_162586/](https://www.consultant.ru/document/cons_doc_LAW_162586/) (Доступ: 05.09.2025).
- Федеральный закон от 06.07.2016 N 374-ФЗ “О внесении изменений в Федеральный закон ‘О противодействии терроризму’ и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_201078/](https://www.consultant.ru/document/cons_doc_LAW_201078/) (Доступ: 19.08.2025).
- Федеральный закон от 06.07.2016 N 375-ФЗ “О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_201087/](https://www.consultant.ru/document/cons_doc_LAW_201087/) (Доступ: 19.08.2025).
- Федеральный закон от 31.12.2017 № 482-ФЗ “О внесении изменений в отдельные законодательные акты Российской Федерации” <https://www.garant.ru/products/ipo/prime/doc/71748784/> (Доступ: 20.08.2025).
- Федеральный закон от 29.12.2022 N 572-ФЗ “Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_436110/](https://www.consultant.ru/document/cons_doc_LAW_436110/) (Доступ: 20.08.2025).
- Федеральный закон от 08.08.2024 N 260-ФЗ “О внесении изменений в отдельные законодательные акты Российской Федерации” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_482512/](https://www.consultant.ru/document/cons_doc_LAW_482512/) (Доступ: 21.08.2025).
- Федеральный закон от 08.08.2024 N 303-ФЗ “О внесении изменений в Федеральный закон ‘О связи’ и отдельные законодательные акты Российской Федерации” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_482565/](https://www.consultant.ru/document/cons_doc_LAW_482565/) (Доступ: 20.08.2025).
- Федеральный закон от 01.04.2025 N 41-ФЗ “О создании государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_502182/](https://www.consultant.ru/document/cons_doc_LAW_502182/) (Доступ: 20.08.2025).
- Федеральный закон от 23.05.2025 N 121-ФЗ (ред. от 31.07.2025) “О внесении изменений в отдельные законодательные акты Российской Федерации и о проведении эксперимента по внедрению дополнительных механизмов учета иностранных граждан” [https://www.consultant.ru/document/cons\\_doc\\_LAW\\_505834/](https://www.consultant.ru/document/cons_doc_LAW_505834/) (Доступ: 20.08.2025).