2024

Государство слежки

Исследование о том, как российское государство с помощью законов и технологий осуществляет цифровое наблюдение

Содержание

Введение

В данном исследовании представлен краткий аналитический обзор того, что происходит в сфере государственного использования технологий слежения в России. Исследование посвящено в основном правовым аспектам и применению существующих правовых норм правоохранительными органами и органами государственной власти, а также их позиции по данному вопросу. Здесь мы делаем обзор существующей нормативно-правовой базы, регулирующей использование таких технологий государственными органами. Кроме того, мы затрагиваем существующие правовые гарантии, вопросы прозрачности и механизмы надзора, предотвращающие злоупотребление такими технологиями со стороны государственных органов.

Сначала мы приводим обзор законов, которые наделяют правоохранительные органы правом прибегать к методам скрытой слежки и использованию соответствующих технологий. Затем,мы перечисляем ряд специальных правовых норм, предусмотренных федеральными законами, которые формируют правовой режим для различных поставщиков информационных услуг. Наконец, мы сосредоточимся на продолжающемся процессе развертывания систем распознавания лиц в общественных местах. Кроме того, мы приводим соответствующую судебную практику ЕСПЧ, освещающую проблемы российской правовой базы по использованию массовой слежки и нарушению права на неприкосновенность частной жизни.

Источники

Когда мы проводили данное исследование, мы опирались как на первичные, так и на вторичные источники. Первичные источники — это оригинальные материалы, содержащие прямые доказательства или информацию из первых рук, такие как федеральные законы, постановления, судебные дела, подзаконные акты, исторические правовые акты (недействующие законы и постановления), законодательные законопроекты и предложения. Первые три дадут представление о существующих правовых основах, критериях, ограничениях использования технологий наблюдения, а также о мерах защиты от возможных злоупотреблений и правоприменительной практике. Два последних помогут нам продемонстрировать динамику и дать ретроспективный взгляд на развитие слежки в Российской Федерации.

Также мы изучаем данные, содержащиеся в общедоступных утечках из госорганов, занимающихся слежкой, а также связанных с ними организаций. Такая информация не будет интерпретироваться сама по себе. Мы сравниваем ее с другими источниками, чтобы сделать вывод о ее точности и достоверности, а также уточнить, что из этого является правдой, а что — вероятной правдой или неправдой. Будет использована только та информация, которая уже является общественным достоянием, а именно обнародована в интернет-СМИ. Соответственно, мы не раскрываем инсайдерскую информацию или не осуществляем доступ к ней самостоятельно.

Вторичные источники интерпретируют или анализируют первичные источники. К таким источникам относятся книги, статьи, в том числе юридические обзоры, в которых обобщаются, критикуются или обсуждаются выводы исследователей. Кроме того, для ознакомления с официальной позицией правительства и мнением экспертов из соответствующих отраслей будут использованы новостные статьи доверенных СМИ.

Кроме того, мы провели ряд интервью с экспертами в области электронных коммуникаций, информационных технологий, инфобезопасности и права для проверки выводов исследования. Каждое интервью проводилось при наличии письменного согласия интервьюируемого, полученного заранее. В согласии оговаривалась политика цитирования, предпочтительная для каждого интервьюируемого. Имена экспертов публично не раскрываются для обеспечения их безопасности

Правовая база, связанная с деятельностью органов государственного надзора по использованию слежки

Законодательство Российской Федерации сильно отличается от законодательства ЕС и обычно рассматривается практикующими юристами как крайне расплывчатое и допускающее широкое толкование со стороны государственных органов.

Ниже мы приводим список законов, которые прямо или косвенно относятся к нашему вопросу:

- Конституция Российской Федерации, принятая 12 декабря 1993 года;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ "О персональных данных" (далее "Закон о персональных данных");
- Федеральный закон от 3 июля 2003 г. № 126-ФЗ "О связи" (далее "Закон о связи");
- Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (далее "Закон об информационных технологиях");
- Административный процессуальный кодекс Российской Федерации от 08.03.2015 № 21-ФЗ;
- Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ;

- Федеральный закон от 02 февраля 2011 г. № 3-ФЗ "О полиции";
- Федеральный закон от 12 августа 1995 г. № 144-ФЗ "Об оперативно-розыскной деятельности";
- Федеральный закон от 12 декабря 2022 г. 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 законодательных актов Российской Федерации" (далее – «Закон о Единой биометрической системе»);
- Федеральный закон от 24 апреля 2020 г. N 123-ФЗ "О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для развития и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона "О персональных данных".

Законодательство о защите неприкосновенности частной жизни

Конституция Российской Федерации предусматривает право на неприкосновенность частной жизни и тайну связи, однако не содержит ни прямых положений, касающихся персональных данных, ни положений, непосредственно связанных с цифровыми правами. Права на неприкосновенность частной жизни и на доступ к своим

персональным данным обеспечены гарантиями, которые закреплены в Конституции.

Во-первых, в части 1 статьи 23 Конституции *закреплено право на неприкосновенность частной жизни, личную и семейную тайну*, защиту чести и доброго имени. Кроме того, часть 2 той же статьи конкретно *предусматривает право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений и ее ограничение по решению суда.* Единственным положением, которое можно считать частично охватывающим обработку персональных данных, является статья 24, предусматривающая, что "*сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются*". Эта статья также предусматривает право на информацию о документах и материалах государственных органов и органов местного самоуправления, непосредственно затрагивающих права и свободы, если иное не предусмотрено законом.

Аналогичные общие положения о тайне связи предусмотрены ст. 63 Закона о связи. Указанная статья гарантирует "тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электросвязи или по почте, если она не может быть ограничена федеральным законом". Данная статья конкретизирует конституционные положения, ограничивая “осмотр почтовых отправлений лицами, не являющимися работниками оператора связи, изъятие почтовых отправлений, осмотр вложений, получение информации и документов, передаваемых по сетям электросвязи и почтовым отправлениям, *за исключением случаев, предусмотренных решением суда или установленных в отдельных случаях федеральным законом*”.

В области защиты персональных данных основным федеральным законом, регулирующим обработку персональных данных, является Федеральный закон от 27 июля 2006 года № 152-ФЗ “О персональных данных”. Указанный федеральный закон был принят в соответствии с такими международными и наднациональными правовыми актами, как Руководящие принципы ОЭСР по защите частной жизни и трансграничных потоков персональных данных, Директива 95/46/ЕС Европейского парламента и Совета от 24 октября 1995 года “О защите физических лиц в отношении обработки персональных данных и о свободном перемещении таких данных” и Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных 1981

года. Последняя была подписана и ратифицирована Российской Федерацией. В 2018 году Россия подписала Протокол о внесении изменений в Конвенцию Совета Европы № 108 о защите физических лиц при автоматизированной обработке персональных данных. Однако в соответствующий федеральный закон не были внесены изменения, а закон о ратификации Протокола о внесении изменений не был принят.

В отличие от GDPR, российский закон о персональных данных характеризуется очень широкой сферой действия, поскольку он охватывает как обработку частными организациями, физическими лицами, так и государственными органами.

Это означает, что общие принципы и правовые нормы применимы как к обработке, осуществляемой с целью получения прибыли или связанной с коммерческой деятельностью, так и к выполнению государственных функций органами государственной власти и местного самоуправления (муниципалитетами). Общие правовые основания для обработки персональных данных установлены ст. 6 Закона. Ниже мы перечислим наиболее актуальные для сферы нашего исследования и применимые правовые основания, которые оправдывают обработку персональных данных в отсутствие согласия субъекта:

- обработка персональных данных осуществляется в связи с участием лица в конституционном, гражданском, административном, уголовном судопроизводстве, судопроизводстве в арбитражных судах;
- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей;
- осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

В ходе судебного разбирательства, ходатайство о раскрытии персональных данных или любых непубличных данных само по себе подлежит судебному рассмотрению. Статья 63 Кодекса административного судопроизводства Российской Федерации от 08.03.2015 № 21-ФЗ предоставляет сторонам процесса право заявлять ходатайства об истребовании доказательств, что в силу широты охвата перечисленных положений и положений Закона о персональных данных, приведенных выше, означает, что персональные данные также могут быть предметом таких ходатайств.

Аналогичным образом ст. 26.10 Кодекса Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ наделяет должностных лиц или органы, а также судей правом направлять запросы о предоставлении информации, необходимой для административного производства. Однако такие ходатайства подлежат судебному рассмотрению, то есть, по общему правилу, запрашиваемая информация (персональные данные) должна иметь отношение к рассматриваемому делу. Тем не менее следует обратить внимание на то, что подобные административные правонарушения в некоторой степени схожи с тем, что в некоторых европейских странах называют уголовными проступками (например, превышать скорость, мусорить, перебегать дорогу и т.д.).

Внесудебный доступ к данным

Одно из упомянутых оснований ст. 6 Закона о персональных данных, а именно обязательное раскрытие или публикация персональных данных в соответствии с федеральным законом, предоставляет государственным органам внесудебный доступ к персональным данным. Некоторые надзорные или правоохранительные органы могут получить доступ к персональным данным без предварительного решения суда.

Прокуратура

Прокуратура, которая также недавно была наделена “цензорскими” полномочиями, ограничивая доступ к веб-сайтам на весьма неопределенных и произвольных основаниях, может получить доступ к персональным данным без предварительного решения суда при условии, что такой доступ необходим для осуществления надзорной деятельности.

Часть 2.1 статьи 4 Федерального закона от 17 января 1992 года № 2202-1 "О прокуратуре" прямо наделяет прокуроров полномочиями по доступу к персональным данным, но только в ходе надзорной деятельности.

Приказ Генеральной прокуратуры от 20 ноября 2013 г. N 506 детализирует некоторые положения рассматриваемого закона, предоставляя неисчерпывающий перечень персональных данных, которые могут обрабатываться прокурорами в ходе надзорных мероприятий.

Однако надзорные полномочия прокурора имеют широкий предметный охват. Закон не ограничивает четко свободу действий прокуроров при осуществлении их полномочий, поскольку не содержит исчерпывающего перечня вопросов. С одной стороны, в нем говорится, что прокуроры несут общую ответственность за соблюдение законов Российской Федерации. С другой стороны, этот же закон устанавливает расплывчатые ограничения их полномочий. Например, в соответствии с Законом на прокуроров возложена задача по обеспечению соблюдения прав и свобод человека, а также соблюдения законов следственными органами и правоохранительными органами, осуществляющими оперативно-розыскную деятельность. Кроме того, в соответствии с ч. 2 ст. 21 и ч. 2 ст. 22 прокуроры не вправе подменять свои правоприменительные полномочия полномочиями других правоохранительных органов. Иными словами, надзорные полномочия прокуроров не должны вступать в конфликт с полномочиями иных государственных органов, прямо предусмотренными федеральными законами. Кроме того, согласно п. 2.3 ст. 6 прокурор не вправе требовать документы и информацию, не связанные с целями и предметом надзора. Практически это означает, что прокуроры должны ссылаться на конкретный федеральный закон, связанный с надзором. И последнее, но не менее важное: прокуроры проводят надзорные мероприятия при наличии информации о нарушении закона или ущемлении прав и свобод человека, полученной от лиц или иных государственных органов.

Полиция

Общие положения правоприменительных полномочий полиции предусмотрены ст. 13 Федерального закона от 02 февраля 2011 г. № 3-ФЗ "О полиции", предоставляющей доступ к персональным данным. Пункты 3 и 5 части 1 указанной статьи наделяют полицию правом "знакомиться с <...> с персональными данными граждан, имеющими отношение к расследованию уголовных дел, производству по делам об административных правонарушениях, проверке заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях".

Закон о персональных данных в п. 11 ч. 1 ст. 6 предусматривает соответствующее правовое основание для обработки персональных данных как *обязательное раскрытие, установленное федеральным законом*. Однако указанная статья Закона о персональных данных не распространяется на чувствительные персональные данные (специальные категории персональных данных в редакции российского законодательства), поскольку ее часть 2 прямо исключает из сферы действия обработку чувствительных и биометрических персональных данных. Две последних категории персональных данных охватываются ст. 10 и ст. 11 Закона о персональных данных, соответственно.

Кроме того, исходя из официальной конструкции Закона о персональных данных Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации, изложенной в информационном письме от 17 июля 2020 г. № ОП-П24-070-19433, в ст. 6 перечислены только общие правовые основания, а ст. ст. 10 и 11 содержат специальные правовые основания для обработки чувствительных и биометрических персональных данных соответственно, которые имеют приоритет перед основаниями, установленными ст. 6 Закона о персональных данных. Согласно ст. 10 обработка персональных данных полицией или другими правоохранительными органами может считаться законной, если она "необходима для защиты жизни, здоровья и иных жизненно важных

интересов субъекта персональных данных или других лиц" либо "для установления или осуществления прав субъекта персональных данных или третьей стороны". Это означает, что сотрудники полиции по-прежнему имеют право доступа к конфиденциальным персональным данным, однако в таком случае юридический порог разумности и обоснованности их запросов выше.

В отношении биометрических персональных данных их обработка является правомерной, если она предусмотрена федеральными законами, указанными в тексте части 2 статьи 11 Закона о персональных данных. В настоящее время только один из федеральных законов, перечисленных в части 2 вышеуказанной статьи, содержит положения, касающиеся обработки биометрических персональных данных. Федеральный закон от 3 декабря 2008 г. N 242-ФЗ "О государственной геномной регистрации в Российской Федерации" предусматривает обязательную геномную регистрацию лиц осужденных и отбывающих наказание в виде лишения свободы за совершение преступлений, а также подозреваемых. Кроме того, с 1 января 2025 года, в силу вступят поправки в указанный закон, согласно которым, помимо прочего лица, подвергнутые административному аресту, также подвергнутся обязательной геномной регистрации.

В остальных случаях мы исходим из такого толкования закона, что сотрудники полиции формально не имеют права запрашивать биометрические персональные данные, поскольку федеральное законодательство прямо не наделяет их такими полномочиями.

Тем не менее здесь следует сделать несколько оговорок. Во-первых, такая точка зрения основана лишь на неофициальном толковании вышеупомянутых федеральных законов. Во-вторых, сфера применения ст. 13 Закона о полиции довольно широка и относится в основном к таким обычным полицейским действиям, как направление запросов и сбора информации или документов в ходе следственной проверки, выемке документов и обыску. Общий характер статьи 13 Закона о полиции охватывает как внесудебный доступ к персональным

данным, когда эти данные не подпадают под защиту, предусмотренную Конституцией или Законом "О связи", так и доступ на основании предварительного судебного решения, когда персональные данные содержат информацию о частной жизни, защищенную вышеуказанными правовыми актами. Иными словами, в ходе различных процессуальных действий сотрудники полиции могут получить прямой доступ к носителям информации, содержащим в том числе биометрические персональные данные, или же запрашивать такую информацию непосредственно у ее обладателя. Примечательно, что факт подачи такого запроса не подлежит конфиденциальности, то есть любая организация, владеющая данными, имеет право сообщить заинтересованному лицу о таких запросах, если только эти запросы не относятся к оперативно-розыскной деятельности.

Согласно пункту 4 статьи 13 Федерального закона "О полиции", а также статьям 6 и 7 Федерального закона "Об оперативно-розыскной деятельности", полиция имеет право получать всю необходимую информацию, включая персональные данные, от любого третьего лица не только при наличии уголовного дела или судебного решения, но и "в связи с проверкой заявлений и сообщений о преступлениях", а также при наличии "признаков противоправного деяния", что представляется весьма расплывчатым понятием. Тем не менее, существующая система запросов информации обязывает поставщиков услуг раскрывать любую информацию, запрашиваемую правоохранительными органами, без возможности проверить наличие достаточных оснований и без какого-либо судебного контроля или надзора со стороны независимого органа по защите персональных данных.

Оперативно-розыскная деятельность

Сотрудники полиции, а также другие правоохранительные органы и органы национальной безопасности (например, ФСБ) имеют иные правовые основания и способы доступа к данным связи и, в частности, к персональным данным.

Основополагающим законодательным актом является *Федеральный закон от 12 августа 1995 г. № 144-ФЗ "Об оперативно-розыскной деятельности"*, который предоставляет правоохранительным органам, уполномоченным на проведение оперативно-розыскных мероприятий, право на сбор и доступ к информации в целом. Согласно широкому определению, данному в ст. 1 указанного закона, «*оперативно-розыскная деятельность вид деятельности, осуществляемой гласно и негласно оперативными подразделениями государственных органов, уполномоченных на то настоящим Федеральным законом (далее — органы, осуществляющие оперативно-розыскную деятельность), в пределах их полномочий посредством проведения оперативно-розыскных мероприятий в целях защиты жизни, здоровья, прав и свобод человека и гражданина, собственности, обеспечения безопасности общества и государства от преступных посягательств*». В ст. 6 исчерпывающе перечислены такие оперативно-розыскные мероприятия, как: опрос, наведение справок, сбор образцов для сравнительного исследования, контрольная закупка, обследование предметов и документов, наблюдение, отождествление личности, осмотр помещений, зданий, сооружений, участков местности и транспортных средств, контроль почтовых отправлений, телеграфных и иных сообщений; прослушивание телефонных переговоров, снятие информации с технических каналов связи, оперативное внедрение, контролируемая поставка, оперативный эксперимент и получение компьютерной информации.

Формально говоря, ст. 5 Закона содержит несколько положений, направленных на обеспечение прав и свобод человека. Прежде всего, *правоохранительные органы обеспечивают неприкосновенность частной жизни, личную и семейную тайну, неприкосновенность жилища и тайну переписки.* Также закон *предоставляет человеку право обжаловать оперативно-розыскные*

мероприятия в отношении него в вышестоящий правоохранительный орган, прокуратуру или суд. Однако для эффективной реализации этого права в суде человек должен иметь в своем распоряжении доказательства того, что в отношении него проводились оперативно-розыскные мероприятия и уголовное расследование в отношении него было прекращено за отсутствием в его действиях преступных событий или деяний. При этом он имеет право на получение информации, собранной о нем в ходе оперативно-розыскных мероприятий, только с соблюдением требований конспирации и государственной тайны. В случае отказа или неполного исполнения такого требования со стороны правоохранительного органа (что встречается довольно часто) человек имеет право обратиться в суд. Если обращение увенчается успехом, суд обяжет правоохранительный орган предоставить истцу информацию, собранную о нем в ходе оперативно-розыскных мероприятий.

Кроме того, указанной статьей предусмотрены правила хранения данных, которые предписывают хранить их в течение 1 года и после этого уничтожать информацию о лицах, вина которых не была установлена. Фонограммы и другие материалы, полученные в результате прослушивания, подлежат уничтожению в течение 6 месяцев с момента прекращения прослушивания, а если такие материалы были получены по решению суда, то соответствующий судья должен быть уведомлен за 3 месяца до уничтожения. Запрещается разглашать без согласия лица сведения, затрагивающие его частную жизнь, личную и семейную тайну, честь и доброе имя, выявленные в ходе оперативно-розыскной деятельности. Если правоохранительным органом или должностным лицом нарушены права и интересы физических или юридических лиц, прокурор или судья обязаны принять меры, направленные на восстановление прав и интересов, и возместить ущерб. Примечательно, что для массовой слежки в ст. 6 содержится исчерпывающий перечень таких оперативно-розыскных мероприятий, применимых к использованию информационных технологий, как контроль сообщений, прослушивание, доступ к компьютерной информации, доступ к информации из каналов связи.

В соответствии со ст. 8 все оперативно-розыскные мероприятия, нарушающие конституционные права на тайну связи, допускаются на основании судебного решения и при наличии информации о:

- готовящихся или совершенных либо совершенных противоправных деяниях, требующих предварительного расследования;

- лицах, подготавливающих, совершающих или совершивших противоправные деяния, требующие в соответствии с законом предварительного расследования;
- событиях, действиях (бездействии), угрожающих государственной, военной, экономической, информационной или экологической безопасности Российской Федерации.

Однако в неотложных случаях, которые могут привести к тяжкому или особо тяжкому преступлению, а также при наличии информации о событиях, действиях (бездействии), угрожающих государственной, военной, экономической, информационной или экологической безопасности Российской Федерации, допускается проведение указанных мероприятий без предварительного судебного решения, при условии уведомления судьи за 24 часа. После начала такой деятельности правоохранительный орган обязан получить судебное решение в течение 48 часов, в противном случае прекратить такую деятельность, однако в соответствии с федеральным законом неполучение соответствующего судебного решения *не влечет за собой удаление, уничтожение или признание недопустимыми доказательствами в суде результатов и результатов такой деятельности.*

Тем не менее следует отметить, что в соответствии со ст. 12.1 Закона содержание запросов о предоставлении информации, поданных в ходе оперативно-розыскных мероприятий, является государственной тайной, то есть получатель запроса не имеет права разглашать его содержание. Кроме того, ст. 12 Закона устанавливает, что *сведения о средствах, источниках, методах, планах и результатах проводимых или проводимых оперативно-розыскных мероприятий, <...> организации и тактике проведения секретных оперативно-розыскных мероприятий составляют государственную тайну и подлежат разглашению только по решению соответствующего органа, осуществляющего оперативно-розыскную деятельность.*

На практике эти две статьи серьезно препятствуют эффективному использованию прав, предусмотренных ст. 5 обсуждаемого Закона и конституционных прав, предусмотренных ст. 24 Конституции РФ. Например, решением Московского городского суда 33а-0672/2021 от 18.02.2021 было отказано в удовлетворении апелляционной жалобы истца на решение суда первой инстанции. Истец обратился в суд с иском к российской полиции,

которая отказалась предоставить ему информацию о проведенных в отношении него оперативно-розыскных мероприятиях. Истец добивался подтверждения самого факта проведения таких мероприятий, информации об их характере, подтверждения проведения служебного расследования в отношении сотрудников, разгласивших информацию, полученную в ходе оперативно-розыскных мероприятий, а также получения копий соответствующих документов. Апелляционная инстанция — Московский городской суд — оставила в силе решение суда первой инстанции и отказала в удовлетворении апелляционной жалобы, подтвердив, что запрашиваемая истцом информация охраняется в соответствии с вышеуказанными статьей 12 как государственная тайна.

Подводя итог, следует отметить, что положения Закона "Об оперативно-розыскной деятельности" прямо наделяют органы полиции и национальной безопасности правом контроля сообщений, прослушивания телефонных разговоров, доступа к компьютерной информации, снятии информации с каналов связи.

Иными словами, указанный закон наделяет ряд правоохранительных органов полномочиями по проведению оперативно-розыскных мероприятий, следовательно, полномочиями по доступу к данным связи и наблюдению за пользователями и абонентами посредством ИКТ (информационно-коммуникационных технологий). Однако положения Закона имеют весьма общую формулировку и разрабатывались в те времена, когда большинство привычных сегодня интернет-сервисов еще не существовало или находилось на начальной стадии своего развития. По этой причине существует ряд федеральных законов и подзаконных актов, облегчающих доступ к данным пользователей Интернета или абонентов услуг связи при проведении оперативно-розыскных мероприятий, которые рассматриваются нами в следующих разделах. Ниже представлен обзор правовых норм, предписывающих технические и организационные требования к организаторам распространения

информации, операторам связи и другим информационным посредникам и поставщикам услуг.

Подводя итог, можно сказать, что российское законодательство, наделяющее государственные органы правоприменительными полномочиями и регулирующее оперативно-розыскную деятельность, имеет следующие особенности:

Закон "Об оперативно-розыскной деятельности":

- существует запрет на разглашение информации об оперативно-розыскных мероприятиях, направленных на получение персональных данных;
- засекреченность (режим государственной тайны) информации, касающейся оперативно-розыскных мероприятий и их результатов, затрагивает права субъекта персональных данных на получение информации об обработке его персональных данных и на доступ к своим персональным данным;
- сложившаяся судебная практика и засекреченный статус (государственная тайна) делает права физических лиц неисполнимыми на практике.

Общие законы, такие как "О полиции", "О прокуратуре", "О персональных данных":

- наличие законодательных положений, предоставляющих государственным органам доступ к персональным данным и другой конфиденциальной информации без предварительного решения суда.

Техническая инфраструктура

Провайдеры цифровых услуг как посредники массовой слежки

Центральным законом, утверждающим так называемое "регулирование новой школы", является Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (далее "Закон об информационных технологиях"). Под "регулированием новой школы" понимается стратегия регулирования, при которой государство делегирует информационным посредникам и провайдерам различных услуг некоторые публичные или правоприменительные функции, обязывая их удалять спорный контент, собирать и хранить данные о своих пользователях и т.д. Указанный закон, помимо информационных ограничений, устанавливает ряд обязательств для различных поставщиков услуг.

В настоящее время следующие поставщики услуг вынуждены заниматься практикой, которая может быть расценена как слежка (ранжированы по степени неблагоприятного воздействия на частную жизнь от высокой до низкой):

- организаторы распространения информации (чаты, форумы, "внутренние" разделы комментариев, мессенджеры);
- хостинг-провайдеры;

- социальные сети;
- сайты объявлений.

Примечательно, что недавняя поправка от 31 июля 2023 года к ст. 8 Закона об информационных технологиях ввела требование для всех российских онлайн-сервисов, доступ к которым осуществляется при условии авторизации пользователя, делать это только с использованием номера мобильного телефона или через государственную систему ЕСИА (Единая система идентификации и авторизации, также известна как “Госуслуги”), или через другую государственную систему, ЕБС (Единая биометрическая система), или через любую другую систему (как государственную, так и частную) при условии, что она не находится под иностранным контролем. Эта же поправка устраняет существовавшую ранее ситуацию, когда хостинг-провайдеры были одними из немногих поставщиков онлайн-услуг, которые по общему правилу не были юридически обязаны участвовать в слежке, например, у них не было исчерпывающих правил идентификации пользователей хостинг-услуг.

Организаторы распространения информации

С принятием Федерального закона от 5 мая 2014 г. № 97-ФЗ (прозванного "Законом о блогерах") была введена ст. 10.1 Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" ("Закон об информационных технологиях"), которая обязывала некоторые коммуникационные сервисы, организаторов распространения информации хранить данные своих пользователей в течение шести месяцев.

В 2016 году в Закон об информационных технологиях были внесены новые изменения в виде принятия Федерального закона от 6 июля 2016 года N 374-ФЗ (прозванного по имени одного из его авторов "пакетом Яровой"), который увеличил срок хранения лог-данных пользователей, то есть метаданных, до одного года, но оставил без изменений шестимесячный срок хранения сообщений пользователей.

Оба типа данных могут быть использованы для наблюдения за пользователями. Однако если метаданные предоставляют в основном статистическую и техническую информацию о подключении пользователя, его устройстве и т. д., то контентные данные содержат сами сообщения, что позволяет властям не только отследить, найти или идентифицировать интересующее их лицо с помощью метаданных, но и использовать эти сообщения в качестве доказательства против него.

В соответствии с Законом об информационных технологиях "Организатор распространения информации" — лицо, осуществляющее деятельность по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети "Интернет". Изучив записи о таких организаторах из соответствующего реестра надзорного ведомства, Роскомнадзора как источника сложившейся практики, можно сделать вывод, что обсуждаемое положение, трактуемое Роскомнадзором, очень широко и включает без ограничений любые веб-ресурсы или приложения, которые позволяют общаться между их пользователями. К числу ресурсов, подпадающих под санкции Роскомнадзора, относятся онлайн-карты или сайты с функцией комментирования или размещения информации, сервисы онлайн-объявлений, банковские приложения с функцией чата и сервисы мгновенного обмена сообщениями.

По сути, статья имеет неадекватно неограниченную сферу применения, которая потенциально может распространяться на любые веб-ресурсы с соответствующим функционалом, независимо от их размера, количества посетителей и способности соответствовать установленным законом требованиям.

Широкий характер статьи приводит к произволу в государственной политике. Естественно, согласно части 3.1 статьи, организаторы распространения информации обязаны раскрывать информацию правоохранительным органам в случаях, установленных федеральным законом.

В настоящее время организаторы распространения информации в соответствии с частью 3 статьи обязаны хранить на территории Российской Федерации следующие пользовательские данные:

- информация о фактах приема, передачи, доставки и (или) обработки

голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей сети Интернет и сведения о них в течение 1 года с момента совершения таких действий (лог дата);

- текстовые сообщения пользователей сети Интернет, голосовая информация, изображения, звуковые, видео или иные сообщения пользователей услуг связи в срок до 6 месяцев с момента их получения, передачи, доставки и (или) обработки (контентные данные).

Детали, касающиеся точного перечня обрабатываемой информации, содержатся в соответствующих актах Правительства РФ, а именно в Постановлении Правительства РФ от 23.09.2020 N1526 и Постановлении Правительства РФ от 26.02.2022 N256, для данных журнала/биллинга и для самих сообщений соответственно. Оба постановления используют так называемый «принцип связи», когда правила хранения данных применяются только к пользователям, осуществляющим доступ через российскую инфраструктуру (а именно к ресурсам, адресам, номерам телефонов, пользователям, имеющим документы, выданные российскими органами власти), или если метаданные указывают на то, что пользователь находится на территории России. Однако в то же время оба постановления обязывают "организатора распространения информации", как он определен в законе, сохранять данные любого пользователя, если правоохранительные органы или органы национальной безопасности уведомят организатора распространения информации о том, что данный пользователь находится на территории России (см. для данных журнала/биллинга: Постановление Правительства РФ от 23.09.2020 N 1526; а для сообщений пользователей — Постановление Правительства РФ от 26.02.2022 N 256). Кроме того, согласно п. 13 Постановления N 1526 организатор распространения информации обязан обеспечить конфиденциальность как самого взаимодействия с органом национальной безопасности, так и предмет этого взаимодействия.

Основным вызывающим беспокойство аспектом такого взаимодействия в контексте массовой слежки является то, что информационные запросы, направляемые органами власти, опираются не только на обычные запросы о предоставлении информации, но и на техническую инфраструктуру, предназначенную для перехвата и извлечения данных, передаваемых через инфраструктуру операторов связи. Такие технические возможности органов власти обеспечиваются ч. 3 ст. 10.1 Закона об информационных технологиях,

которая обязывает организаторов распространения информации:

- устанавливать оборудование и программно-технические средства наблюдения и соблюдать соответствующие технические требования, а также принимать меры по предотвращению разглашения организационных и тактических приемов его установки;
- раскрывать ключи шифрования (или любую другую информацию, необходимую для дешифрования) органам власти, если организатор использует дополнительное шифрование или предоставляет пользователям такую возможность.

Технические возможности оборудования для наблюдения описаны в Приказе Министерства связи и массовых коммуникаций Российской Федерации от 29 октября 2018 г. N 571 (в ред. Приказа Министерства связи и массовых коммуникаций Российской Федерации от 28 августа 2023 г. N 750).

Одним словом, оборудование, предназначенное для доступа ко всей указанной в настоящем подразделе информации по каналам связи при проведении оперативно-розыскных мероприятий, фактически обеспечивает сотрудникам ФСБ удаленный, устойчивый, в действительности неконтролируемый, бесперебойный и круглосуточный доступ к информации с минимальной задержкой (от 2 секунд до 5 минут для определенных данных), а также предоставляет непрямой и достаточно ограниченный доступ для других правоохранительных органов.

Согласно упомянутым в этом подразделе постановлениям, удаленный доступ к такому оборудованию имеют только и исключительно территориальные управления ФСБ. Поэтому полиция и другие правоохранительные органы прибегают к более распространенному прямому запросу предоставления информации, в противном случае они вынуждены сотрудничать с ФСБ для получения нужной им информации. Отметим, что это оборудование является

лишь частью СОРМ (Системы оперативно-розыскной деятельности) 3-го поколения. СОРМ — государственная техническая инфраструктура, позволяющая осуществлять прослушивание и перехват сообщений, интегрированная в сети операторов связи и некоторых поставщиков IT-услуг.

В случае с организаторами распространения информации мотивом установки такого оборудования является предоставление правительству возможности не только перехватывать коммуникации, осуществляемые через стационарные или мобильные сети, но и коммуникации, опосредованные различными веб-сайтами и платформами обмена сообщениями.

Как было сказано выше, определение организатора распространения информации довольно широкое, что обуславливает большую степень свободы действий при применении обсуждаемой статьи. В настоящее время под надзор соответствующих надзорных органов попадают только сервисы, предлагающие любые коммуникационные функции, включая, но не ограничиваясь размещением сообщений, комментированием или общением в чате. Однако риск того, что сфера применения статьи может быть расширена, все же существует, поскольку она во многом зависит от толкования Роскомнадзором Закона об информационных технологиях.

Степень соблюдения закона зависит от местонахождения организаторов распространения информации и их неформальных отношений с представителями власти. Такие организаторы распространения информации, как WhatsApp и Telegram, не соблюдают требования закона и, предположительно, не желают активно сотрудничать с правоохранительными органами, насколько можно судить по тому, что WhatsApp даже не находится в соответствующем государственном реестре (существует более удобная копия реестра, поддерживаемая и обновляемая автоматически правозащитниками из организации "Роскомсвобода"), а для соблюдения закона требуется установка специализированного оборудования. Судя по имеющейся информации, крайне маловероятно, что WhatsApp и Telegram приобрели бы и установили такое оборудование в России. Наконец, сотрудничество между WhatsApp и властями может быть маловероятным с политической точки зрения: материнская компания приложения сервиса для обмена сообщениями, Meta Inc., была объявлена в России экстремистской организацией и внесена в соответствующие реестры Минюста и Росфинмониторинга. Кроме того, применение сквозного шифрования позволяет скрыть содержимое сообщений от повсеместного СОРМ

и значительно снижает ценность потенциального сотрудничества между операторами связи и правоохранительными органами. Насколько нам известно, расшифровка сообщений невозможна, поэтому правоохранительные органы прибегают к сбору метаданных или журналов звонков, совершенных через сервисы обмена сообщениями.

Российские организаторы распространения информации, напротив, проявляют большую готовность к сотрудничеству с правоохранительными органами, игнорируя иногда процедурные правила обработки законных запросов на получение информации от правоохранительных органов. Например, социальная сеть и организатор распространения информации VK (“Вконтакте”), как сообщается, несколько раз нарушила все процессуальные нормы и раскрыла данные своих пользователей по запросу, в котором не указывались достаточные основания и не говорилось о ведущемся расследовании преступления или доследственной проверке. Попытки привлечения социальной сети к ответственности не увенчались успехом. Кроме того, сообщалось о нескольких случаях, когда VK предоставлял информацию по неофициальным запросам полиции, отправленным просто по электронной почте.

Хостинг-провайдеры

Последние изменения в Закон об информационных технологиях, внесенные Федеральным законом от 31 июля 2023 года N 406-ФЗ, содержат новую статью 10.2-1, устанавливающую новые правила именно для хостинг-провайдеров, которым до сих пор в целом удавалось избежать соблюдения требований, предъявляемых к организаторам распространения информации.

Хостинг-провайдер в соответствии с определением, данным в ст. 2 Закона об информационных технологиях, является лицо, предоставляющее вычислительные мощности для загрузки информации в информационную систему, постоянно подключенную к сети Интернет, например, GoDaddy Inc., Amazon Web Services. Требования вновь принятых положений касаются всех хостинг-провайдеров, имеющих связь с территорией России, либо обрабатывающих данные российских пользователей, либо получающих деньги от российских пользователей, либо предоставляющих услуги хостинга на российском рынке.

Части 3 и 5 статьи 10.2-1 налагают на хостинг-провайдеров новые обязательства, включая установку оборудования для наблюдения и идентификацию пользователей услуг хостинга соответственно. Ни та, ни другая части не содержат каких-либо подробностей относительно предмета и технических требований, а также того, какие данные должны храниться и каков срок хранения этих данных. Именно Приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 1 ноября 2023 г. N 935 устанавливает трехлетний срок хранения данных о своих клиентах, то есть пользователях услуг хостинга, (в т.ч. журналы, биллинг, геолокация, персональные данные), и однодневный срок хранения данных о взаимодействии клиентов услуг хостинга с другими пользователями Интернета, а также описывает технические возможности оборудования для слежки. Следует обратить внимание, что правила для хостинг-провайдеров предусмотрены

вышеупомянутым Приказом, который является подзаконным актом, в отличие от правил хранения данных, установленных федеральным законом для организаторов распространения информации. Другими словами, не нужно проходить через законодательную волокиту, поэтому изменить объем и срок хранения данных для хостинг-провайдеров гораздо проще и быстрее, чем для организаторов распространения информации.

Идентификация пользователей услуг хостинга подробно прописана в Постановлении Правительства РФ от 29.11.2023 N 2011 31 июля 2023 года и, помимо некоторых дополнительных способов идентификации, в целом соответствует ст. 8 Закона об информационных технологиях, поскольку предписывает, что идентификация и (или) аутентификация пользователей должны осуществляться с использованием российской информационной или финансовой инфраструктуры.

В заключение следует отметить, что созданная инфраструктура и вновь принятые соответствующие законодательные требования способствуют дальнейшему развитию системы СОРМ. Аналогично организаторам распространения информации в территориальных подразделений Федеральной службы безопасности установлены так называемые панели управления, обеспечивающие такой же неограниченный доступ к информации и функции поиска и копирования.

Операторы связи, СОРМ

В данном подразделе мы рассмотрим прослушивание телекоммуникационных каналов, то есть только наблюдение за абонентами, получающими телекоммуникационные услуги от операторов связи — юридических лиц или индивидуальных предпринимателей, предоставляющих услуги связи на основании лицензии, таких как операторы мобильной или стационарной связи, провайдеры доступа в Интернет, провайдеры спутниковой связи и т. д.

Ст. 64 Федерального закона № 126-ФЗ "О связи" создает правовую основу для доступа государственных органов к персональным данным через операторов связи. С 2016 года, когда был принят "пакет Яровой", согласно этой статье, оператор связи обязан хранить на территории Российской Федерации:

- информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи в течение 3 лет с момента совершения таких действий;
- текстовых сообщений пользователей услуг связи, голосовой информации, изображений, звуковых, видео- или иных сообщений пользователей услуг связи — до 6 месяцев.

Существует обязанность операторов связи сотрудничать со следственными органами, предоставляя им информацию о своих пользователях, оказываемых услугах и другую информацию. Технической инфраструктурой, обеспечивающей прослушивание телефонных разговоров, является СОРМ, которая пережила несколько поколений.

СОРМ-1 позволяла вести наблюдение за телефонными переговорами и была построена еще в 1996 году. Она предполагала установку в инфраструктуру оператора мобильной или стационарной связи устройств, которые записывали телефонный трафик и разговоры и предоставляли правоохранительным органам доступ к этим записям.

СОРМ-2 была создана для прослушивания мобильной связи и, конечно же, контроля над Интернетом. СОРМ-2 — это система хранения информации об интернет-трафике, разработанная в 2000 году совместно ФСБ России и предшественниками Роскомнадзора, но окончательно развернутая только в 2008 году. В ее основе лежало специальное оборудование, установленное на территории провайдера и за его счет, которое хранит весь трафик, передаваемый по сетям провайдера, и предоставляет правоохранительным органам доступ к этому хранилищу.

СОРМ-3, самая последняя версия, обеспечивает интеграцию всех вышеперечисленных систем и дополнительный контроль над некоторыми VPN-серверами, прослушивание Skype, данных коммуникаций из сервисов обмена сообщениями предлагающих шифрование (например, WhatsApp, Telegram, Signal), спутниковой связи и ряд других возможностей. Хотя стоит отметить, что доступ к службам обмена сообщениями, использующим сквозное (e2e) шифрование, ограничивается метаданными. Но главный результат внедрения СОРМ-3 состоит в том, что он объединил предыдущие поколения СОРМ. Основные особенности заключаются в обеспечении круглосуточного, в режиме реального времени, неизбирательного доступа к коммуникационным данным, включая данные об абонентах, содержание сообщений, если они не зашифрованы, данные регистрации и биллинга, геолокационные данные.

Приказ Министерства связи и массовых коммуникаций Российской Федерации от 29.10.2018 N 573 устанавливает технические требования ко всей системе СОРМ, объем наблюдения и т. д. Последние изменения от сентября 2023 года включили в сферу наблюдения VoWiFi, WiFi Calling. Другой нормативный акт, Приказ Министерства связи и массовых коммуникаций Российской Федерации от 16.04.2014 N 83, устанавливает правила прослушивания интернет-коммуникаций путем установки на стороне операторов связи специального оборудования, предназначенного для сбора данных о соединении

(IP и MAC-адреса, IMEI и т.д.) и содержании сообщений пользователя.

Вся эта система позволяет правоохранительным органам получать доступ практически ко всем данным, передаваемым через телекоммуникационных провайдеров или каналы связи, без ведома пользователей и операторов связи.

Специальное оборудование функционирует на постоянной основе (круглосуточно) в автоматическом режиме или по запросу и контролируется исключительно Федеральной службой безопасности (ФСБ), органом национальной безопасности. Система СОРМ предназначена для доступа к информации по каналам связи в ходе проведения оперативно-розыскных мероприятий, что обеспечивает стабильный и бесперебойный доступ к информации через операторов связи без ведома импортера данных.

Однако отсутствие нормативных гарантий, а также практическая реализация самой системы способствуют злоупотреблению использования СОРМ. Как мы уже упоминали в разделе 4 Главы 1, посвященном оперативно-розыскным мероприятиям, лицо, подвергшееся таким мероприятиям, не имеет возможности воспользоваться своим конституционным правом на информацию, поскольку информация об оперативно-розыскных мероприятиях является государственной тайной и решение о том, раскрывать ее или нет, принимает правоохранительный орган. Возможность прослушивать коммуникации с помощью системы в любое время делает существующий судебный надзор практически неэффективным и несуществующим, поскольку сотрудники ФСБ могут использовать ее в любое время, не получая разрешения суда, если только они не хотят представить данные из СОРМ в качестве доказательства по уголовному делу. Хотя и в этом случае они имеют право собирать доказательства без предварительного разрешения суда.

Один из наших источников сообщил довольно тревожные подробности о реальном использовании системы.

Панели управления СОРМ, установленные на территории ФСБ, предоставляют т.н. root-доступ к системе, то есть ФСБ имеет полный технический доступ к панели управления, что означает, что агенты ФСБ могут удалять и даже изменять данные логов и историю сделанных ими запросов, тем самым усугубляя общую непрозрачность слежки, осуществляемой с помощью СОРМ.

Это означает, что сотрудники ФСБ могут напрямую прослушивать коммуникации, не подавая ходатайств о получении разрешения суда. Мы поинтересовались у источника, существуют ли какие-либо внутренние меры по обеспечению подотчетности или соответствия. Как пояснил наш источник, существует лишь сугубо внутренний документ, устанавливающий прокурорский надзор за использованием системы СОРМ. Однако, поскольку он никогда не был обнародован, его содержание неизвестно, равно как и случаи, когда прокуроры вмешивались в использование системы СОРМ.

Что касается прослушивания в целом и того, как различные правоохранительные органы решают задачу перехвата сообщений или сбора информации об интересующем их лице, наш источник указал на три распространенных сценария. В следующих пунктах мы приводим информацию, которой они поделились с нами.

Первый сценарий — ФСБ проводит собственные оперативно-розыскные мероприятия с использованием панели управления СОРМ, делая отдельные целевые запросы о пользователях или активно прослушивая их каналы связи. Как правило, техническим наблюдением и эксплуатацией контрольных панелей СОРМ занимаются технические подразделения местных управлений ФСБ. Существует внутренняя процедура, когда рядовой сотрудник подает официальный запрос в техническое подразделение, поэтому теоретически существует возможность внутреннего контроля слежки. Однако нам стало известно, что иногда сотрудники практикуют неофициальные запросы без соблюдения внутренней процедуры, подходя к коллегам из технического отдела с неформальной просьбой получить определенную информацию, прослушать

объект или просто взглянуть на экран. Наш источник также отметил, что именно в таких случаях root-доступ к панели управления СОРМ помогает скрыть подобные неформальные запросы.

Второй сценарий описывает ситуацию, когда сотрудники полиции, проводящие собственные оперативно-розыскные мероприятия или расследование, имеют доступ к коммуникационной информации. Исходя из общедоступной информации, принято считать, что технические возможности Министерства внутренних дел (МВД) ниже, чем у ФСБ, поэтому у сотрудников полиции обычно есть два варианта: они могут либо сотрудничать с ФСБ, чтобы получить информацию, собранную с СОРМ, либо напрямую запрашивать информацию у операторов связи. В последнем случае отследить такую деятельность несложно, поскольку сами запросы на получение информации регистрируются обеими сторонами. Кроме того, в последнем случае всегда есть некоторая задержка, так как требуется некоторое время на обработку запросов и их выполнение, по этой причине обычные запросы на информацию не могут быть эффективной заменой СОРМ. Очевидно, что благодаря техническим возможностям контрольных панелей СОРМ сотрудники ФСБ имеют наиболее широкий доступ к данным связи, однако, например, сотрудники полиции при составлении запросов на получение информации, направляемых непосредственно операторам связи, полагаются либо на возможности ФСБ, прибегая к СОРМ, либо на опыт собственных сотрудников. В последнем случае это означает, что глубина и объем запроса на информацию зависят от квалификации и опыта сотрудника полиции, составляющего запрос. Однако эксперт обратил наше внимание на то, что существует такая практика, когда некоторые сотрудники полиции не соблюдают процессуальные требования, иногда устанавливая неофициальные, неформальные отношения с коррумпированными сотрудниками телекоммуникационных компаний, чтобы незаконно получить доступ к интересующим их данным. Естественно, телекоммуникационные компании не публикуют отчеты о прозрачности, раскрывающие количество запросов на получение информации, как было указано в Главе 1, и даже простой запрос, сделанный в ходе оперативно-розыскных мероприятий, является предметом требований конфиденциальности.

Третий сценарий частично совпадает со вторым. Центральный мотив этого сценария — злоупотребление властью даже не для того, чтобы облегчить себе

службу, а чтобы заработать деньги на стороне. Это тот случай, когда все пороки системы используются, в особенности сотрудниками полиции, для получения взяток за такие теневые услуги, как сбор информации об изменах супругов, конкурентах, потенциальных жертвах шантажа и т. д. Иногда они контактируют не напрямую с заказчиками таких противоправных действий, а с посредниками — частными детективами, сотрудниками охранных предприятий или внутренней безопасности, которые нередко сами являются бывшими полицейскими или сотрудниками иных правоохранительных органов. Естественно, сотрудники не соблюдают процессуальные требования и не оформляют документы, по которым можно отследить их незаконную деятельность. При таком раскладе использование СОРМ сотрудниками полиции маловероятно, поэтому для получения интересующей их информации они пользуются неформальными контактами среди операторов связи или используют различные веб-сервисы.

Полномасштабная прослушка по первому сценарию чаще всего используется только в громких делах (как уголовных, так и политических) из-за нехватки времени и средств. Источник пояснил, что сотрудники правоохранительных органов, а именно полиции, преследуя людей за свободу слова или собраний, больше полагаются на сбор метаданных, которые в итоге помогают им приблизительно определить местоположение пользовательского устройства и, соответственно, самого пользователя. После этого полицейские проводят обычные оперативные мероприятия, такие как обыски или посещения предполагаемых мест нахождения пользователей. Источник отметил, что прослушка, перехват данных о содержимом, в таких случаях практикуется редко, если вообще практикуется.

Своим путем: СОРМ и международное право

В 2015 году ЕСПЧ в своем решении по делу «Роман Захаров против России» единогласно признал, что право на неприкосновенность частной жизни, гарантированное статьей 8 Европейской конвенции по правам человека 1950 года, было нарушено, и установил, что внутрироссийские правовые нормы, регулирующие перехват сообщений, не обеспечивают адекватных и эффективных гарантий от произвола и риска злоупотреблений.

Суд постановил, что внутреннее законодательство не отвечает требованию "качества закона" и не способно ограничить "вмешательство" тем, что оно "необходимо в демократическом обществе" (п. 304). Несмотря на то, что решение было вынесено в отношении наблюдения за мобильной телефонной связью, выводы суда актуальны и сегодня, а параллели можно провести с наблюдением за интернет-коммуникациями, поскольку оба вида тайного наблюдения имеют одинаковую правовую базу (федеральное законодательство) и осуществляются одними и теми же правоохранительными органами.

Суд пришел к выводу, что риск злоупотреблений, присущий любой системе тайного наблюдения, был особенно высок в России, где секретные службы и полиция имели прямой доступ с помощью технических средств ко всем мобильным телефонным сообщениям.

Суд обнаружил недостатки в правовой базе в следующих областях: обстоятельства, при которых государственные органы в России имеют право

прибегать к мерам тайного наблюдения; продолжительность таких мер, в частности, обстоятельства, при которых они должны быть прекращены; процедуры выдачи разрешения на перехват, а также хранения и уничтожения перехваченных данных; надзор за перехватом (п. 302).

Кроме того, эффективность средств правовой защиты, доступных для оспаривания перехвата сообщений, была подорвана тем фактом, что зачастую заявитель не может представить доказательства такого перехвата

Это вытекает из ст. 5 Закона "Об оперативно-розыскной деятельности", и что получение таких доказательств было невозможно в отсутствие какой-либо системы уведомлений или возможности доступа к информации о перехвате в силу ее засекреченного статуса.

В заключение следует отметить, что данное постановление ЕСПЧ установило, что законодательство и практика Российской Федерации имеют следующие особенности:

- Внутреннее законодательство недостаточно ясно сформулировано, чтобы дать лицам адекватное представление о том, при каких обстоятельствах и на каких условиях государственные органы имеют право прибегать к тайному наблюдению в рамках оперативно-розыскной деятельности, а не к другим, менее навязчивым действиям;
- Принцип необходимости и соразмерности не соблюдается, поскольку законодательство, а именно Закон об информационных технологиях и Закон о связи, разрешило на обобщенной основе хранение всех персональных данных всех лиц без объективного критерия, установленного в законодательстве для определения пределов доступа государственных органов к данным и их последующего использования, в целях, которые являются конкретными, строго ограниченными и способными оправдать вмешательство, которое влечет за собой как доступ к данным, так и их использование;

- Отсутствие независимого (в том числе внесудебного) механизма надзора. Лица имеют право подать жалобу только в правоохранительный орган, проводивший оперативно-розыскные мероприятия в соответствии со ст. 5 Закона "Об оперативно-розыскной деятельности";
- Эффективные средства правовой защиты недоступны. Жалобы на оперативно-розыскные мероприятия в нарушивший орган или иск о том, что персональные данные были получены в ходе оперативно-розыскных мероприятий, не будут поддержанны, так как заявитель не может получить доказательства в поддержку своих требований и эффективно защитить свои права.

Выводы ЕСПЧ по делу «Роман Захаров против России» показывают, что российская правовая база, попустительствующая широко распространенной практике скрытой массовой слежки за коммуникациями, нарушает статью 8 Европейской конвенции по правам человека.

Более того, эта же правовая база не позволяет эффективно ограничивать доступ государственных органов к данным о коммуникациях в той степени, которая необходима и соразмерна демократическому обществу, и не обеспечивает субъектам данных эффективное (принудительное) возмещение ущерба.

В заключение следует отметить, что российское государство не только отказалось выполнять ключевые выводы ЕСПЧ, но и Федеральное собрание (российский парламент) приняло федеральный конституционный закон, наделяющий Конституционный суд РФ правом определять возможность исполнения решения любого межправительственного органа по правам и свободам человека, если существует неопределенность в его соответствии Конституции.

Еще одно примечательное дело ЕСПЧ, касающееся использования СОРМ государственными органами, — «Подчасов против России» (дело о ключах шифрования Telegram), в котором рассматривались именно правовые требования к организаторам распространения информации, установленные ч. 3 ст. 10.1 Закона об информационных технологиях, а именно: требование установить оборудование для слежки, обеспечивающее доступ к данным, и передать ключи шифрования в ФСБ. Это решение ЕСПЧ было основано на упомянутом выше деле «Роман Захаров против России», поскольку правовые основы тайного наблюдения и его осуществления, как признал ЕСПЧ, одинаковы как для поставщиков телекоммуникационных услуг, так и для организаторов распространения информации (п. 55).

И вновь ЕСПЧ единогласно признал, что право на защиту неприкосновенности частной жизни, гарантированное статьей 8 Европейской конвенцией по правам человека 1950 года, было нарушено. Суд отметил, что оспариваемые положения преследовали законную цель, но оспариваемое законодательство не было необходимым в демократическом обществе. Отсутствие правовых гарантий, таких как отсутствие законного требования к правоприменителям "в соответствии с внутренним законодательством предъявлять судебное разрешение поставщику услуг связи перед получением доступа к коммуникациям лица" (п. 72), обязанность устанавливать аппаратное оборудование, позволяющее получать прямой удаленный доступ ко всем интернет-коммуникациям и связанным с ними данным, обосновывало довод о том, что такое вмешательство не является необходимым в демократическом обществе. ЕСПЧ пришел к выводу, что "российская [правовая система], позволяющая спецслужбам получать прямой доступ к интернет-коммуникациям каждого гражданина, не требуя предъявления разрешения на перехват ни поставщику услуг связи, ни кому-либо еще, особенно подвержена злоупотреблениям" (п. 72). Рассматривая положение, обязывающее организаторов распространения информации расшифровывать данные, суд пришел к выводу, "*что в данном случае <...> законодательное обязательство расшифровывать сквозные зашифрованные сообщения рискует оказаться равносильным требованию, чтобы поставщики таких услуг ослабили механизм шифрования для всех пользователей; соответственно, оно не соразмерно преследуемым законным целям*" (п. 79). Суд исходил из того, что технически не существует возможности обеспечить дискриминационный доступ к зашифрованным сообщениям, т.е. доступ к конкретным пользователям Telegram, представляющим интерес, вместо

этого российская законодательная база предусматривает обратное — неограниченный доступ к сообщениям и другим данным всех пользователей пытаясь ослабить шифрование для всех пользователей (п. 77).

Биометрия и распознавание лиц

В настоящее время не существует федеральных законов, которые бы прямо регулировали использование распознавания лиц правительством. Не существует и федеральной системы распознавания лиц.

Хотя есть инициативы по созданию общегосударственной базовой инфраструктуры и инструментария для других субъектов Федерации, который поможет местным органам власти развернуть системы распознавания лиц. Общее количество видеокамер в России, по словам профильного министра Максута Шадаева, насчитывает более 1 миллиона. При этом каждая третья камера видеонаблюдения подключена к системам распознавания лиц.

Правовые основы использования системы распознавания лиц в общественных местах прямо не установлены федеральным законодательством. С одной стороны, ч. 1 ст. 11 Закона о персональных данных содержит общий правовой запрет на обработку биометрических персональных данных без согласия субъекта персональных данных. Часть 2 той же статьи содержит исчерпывающий перечень исключение, когда обработка биометрических данных может быть использована без согласия субъекта персональных данных. В настоящее время правительство, похоже, полагается на пару исключений для осуществления массовой слежки с использованием технологий AI/ML в сочетании с обработкой биометрических данных. Эти исключения касаются борьбы с терроризмом и безопасности на транспорте.

Однако в соответствующих федеральных законах нет ни четких положений, касающихся биометрических персональных данных, ни четких отступлений, позволяющих правительству обрабатывать биометрические персональные данные в соответствии с этими федеральными законами. В этой главе упоминается несколько примеров эффективного, де-факто, использования технологий распознавания лиц — на транспорте и в некоторых государственных школах. В последнем случае системами распознавания лиц должны быть оснащены только государственные спортивные школы, а также спортивные

сооружения в целом, имеющие на своей территории так называемые объекты повышенного риска террористических атак, которые могут привести к жертвам более 101 человека (например, стадионы, бассейны и другие подобные объекты).

Распознавание лиц: продолжающийся правовой эксперимент.

Еще одним актом федерального законодательства, который косвенно дает правовые основания для локального использования системы распознавания лиц, является Федеральный закон от 24 апреля 2020 г. N 123-ФЗ "О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для развития и внедрения технологий искусственного интеллекта в субъекте Российской Федерации - городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона "О персональных данных". Данный закон фактически косвенно наделяет органы власти города федерального значения Москвы полномочиями по использованию технологий распознавания лиц на территории Москвы.

А именно: пункт 5 части 1 ст. 4 указанного закона можно охарактеризовать как установление обязательных требований к раскрытию информации путем наделения исполнительных органов местного самоуправления полномочиями: "устанавливать порядок и случаи передачи владельцами средств и систем фото- и видеонаблюдения изображений, полученных в соответствии с условиями, предусмотренными подпунктами 1 и 2 пункта 1 статьи 152.1 Гражданского кодекса Российской Федерации (изображения лиц, сделанные в общественных интересах либо в общественных местах или на публичных мероприятиях), а также предоставления доступа к таким средствам и системам фото- и видеонаблюдения государственным органам и организациям, выполняющим публичные функции в соответствии с нормативными правовыми актами Российской Федерации".

В настоящее время не существует единого правила такой передачи и предоставления доступа, а также определенного целевого назначения, что оставляет государственным органам большую свободу действий. В соответствии с Постановлением Правительства Москвы от 3 декабря 2020 г. N 2136-ПП такое взаимодействие осуществляется в каждом конкретном случае на условиях, предусмотренных договорами между Департаментом информационных технологий Правительства Москвы и владельцами средств фото- и видеонаблюдения. Кроме того, в соответствии с данным постановлением вся передача изображений и предоставление доступа должны осуществляться через государственную информационную систему "Единый центр хранения и обработки данных".

Примечательно, что такая обработка персональных данных (изображений) строго не противоречит общему запрету, установленному ст. 11 Закона о персональных данных. Фактически простые изображения физических лиц не считаются биометрическими персональными данными, если они не используются для идентификации субъекта персональных данных. Такое толкование вытекает из самого закона, а именно из определения биометрических персональных данных, приведенного в ч. 1 ст. 11 Закона о персональных данных и полностью поддерживается надзорными органами, Минцифры и судебной практикой.

Даже в Москве процесс принятия и внедрения технологии распознавания лиц в целом занял достаточно продолжительное времени. Местные власти годами создавали соответствующую инфраструктуру, прежде чем стало возможным простое тестирование технологий распознавания лиц. Например, в этот период, в 2012 году, московские власти создали Единый центр хранения и обработки данных (ЕЦХД) — центральное хранилище видеоданных с удаленным доступом к камерам и архивам в режиме реального времени.

С 2016 по 2018 год технология распознавания лиц тестировалась в рамках развития городских программ общественной безопасности, в том числе при подготовке к Чемпионату мира по футболу, который проходил в России в 2018 году. Учитывая доступные публичные заявления высших должностных лиц, общегородское внедрение ИИ, похоже, началось в какой-то момент в 2019 году.

В городе также была реализована программа "Безопасный город", которая объединила на единой платформе все системы, отвечающие за безопасность

общественного транспорта, базы данных полиции, информационные системы Минздрава и МЧС, а также системы регионального уровня, уровня административных округов и муниципальных районов.

Таблица 1 — Краткая хронология развития видеонаблюдения, предшествующая московскому эксперименту с искусственным интеллектом. Строка с 2022 годом была добавлена нами. Оригинальная таблица, а также более подробный анализ развития распознавания лиц, см.: Ross, Serebrennikov and others. Surveillance Technologies in Autocratic Regimes: The Moscow AI Experiment and its Implications for Crime Control and Police Effectiveness

2001	Черно-белые камеры в жилых домах и общественных местах
2005	Подключение камер к пунктам видеонаблюдения
2007	Запуск программы "Безопасный город
2010	Создан Департамент информационных технологий Москвы; назначен новый мэр Сергей Собянин
2011	Создан Единый центр хранения данных; рост числа протестов
2012	Запрет на сокрытие лица на митингах
2014	Развитие программы "Безопасный город”
2015	Принятие антитеррористических мер к чемпионату мира по футболу 2018 года
2016	NtechLab представила технологию FindFace
2017	Начало сотрудничество Департамента информационных технологий Москвы с NtechLab
2018	Тестирование системы распознавания лиц для чемпионата мира по футболу 2018 года
2019	Сотрудничество Сбербанка и правительства Москвы

2020	Запуск эксперимента с искусственным интеллектом; использование наблюдения для отслеживания граждан во время пандемии COVID-19
2021	Получение ЕБС статуса ГИС (государственная информационная система), установление государственной монополии на биометрические данные
2022	Использование технологий против протестующих и лиц, уклоняющихся от военной мобилизации

Так называемый легальный эксперимент с общегородским использованием AI/ML начался в 2020 году. Внедрение технологии в городе совпало с глобальной пандемией COVID-19. В январе 2020 года правительство Москвы закупило технологии распознавания лиц у компаний KtechLab (частично принадлежит госкорпорации Ростех), Visionlabs (дочерняя компания Сбербанка) и Tevian. В конце 2020 года правительство Москвы приняло несколько постановлений, которые официально узаконили использование технологий AI/ML в Московском городском округе и обеспечили поступление данных изображений из частных систем видеонаблюдения (см.: Постановление Правительства Москвы от 03.12.2020 N 2136-ПП "О порядке и случаях передачи собственниками средств и систем фото- и видеонаблюдения изображений, а также предоставления доступа к средствам и системам фото- и видеонаблюдения в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в городе Москве" // Вестник Мэра и Правительства Москвы", N 69, 15.12.2020).

Однако ни в одном из постановлений Правительства Москвы нет прямого указания на использование ИИ для распознавания лиц.

В Москве прошло несколько крупных политических митингов, общей особенностью которых стало то, что многие участники были задержаны после

них. По данным ОВД-Инфо, за неделю после митинга 23 января 2021 года было задержано около 100 человек. При этом на самом митинге было задержано 212 человек. Всего ОВД-Инфо зафиксировало не менее 454 задержаний постфактум в 2021 году. Из них 363 связаны с митингом 21 апреля. Не менее 164 человек отметили, что во время общения с полицией или в ходе судебных заседаний им рассказывали об использовании фото- и видеоматериалов в качестве судебных доказательств.

Сегодня есть предположение, что все камеры видеонаблюдения на московском транспорте и значительная часть камер на общественных улицах подключены к Единому центру хранения и обработки данных. В московском метрополитене системы распознавания лиц используются в правоохранительной деятельности и для бесконтактных платежей. Первая система получила официальное название "Сфера". Кроме того, в апреле 2023 года военный комиссар Москвы заявил, что система распознавания лиц используется для поиска призывников. Помимо транспортной инфраструктуры и улиц Москвы, местные власти планировали запустить систему распознавания лиц в московских государственных школах.

Главной проблемой использования системы распознавания лиц в Москве является полная непрозрачность процедуры сбора эталонных изображений, а также их последующего использования для идентификации. Такие эталонные фотографии могут быть получены автоматически из профилей пользователей, зарегистрированных на сайте mos.ru, поскольку разработка такого функционала заказывалась местными властями. Более того, в связи с общим запретом на обработку персональных данных, о котором знают власти, они вынуждены прибегать к ухищрениям при толковании и формальностям, чтобы избежать обязанности соблюдать закон. Такая формальность была выявлена в деле Алены Поповой в 2019 году.

В конце 2018 года Алена Попова провела одиночный пикет у здания Госдумы с требованием отставки депутата Леонида Слуцкого, который предположительно сексуально домогался до нескольких журналисток. За этот поступок она была привлечена к административному штрафу в размере 20 000 рублей. В деле обвинения были представлены изображения с камеры видеонаблюдения, проанализированные с помощью технологии распознавания лиц. В 2019 году Алена Попова попыталась оспорить использование изображений, полученных с помощью общественных видеокамер, и применение технологии распознавания

лиц. Она подала административный иск к ГУ МВД и Департаменту информационных технологий правительства Москвы, но в итоге и суд первой инстанции, и апелляционный суд отклонили ее дело. Если опустить доводы суда об использовании просто изображений людей (т.е. необработанных изображений без какой-либо дополнительной информации), то именно объяснение местных властей об отсутствии обработки биометрических персональных данных послужило основанием для прекращения дела. Суд лишь подтвердил правовую позицию правительства Москвы: "*Алгоритм распознавания лиц, используемый ЕЦХД, сравнивает изображение, полученное ЕЦХД с видеокамер, с фотографией, предоставленной правоохранительным органом. В процессе обработки соответствующие изображения сравниваются на предмет наличия или отсутствия совпадений. Департамент не передает персональные данные (ФИО и т.д.) разыскиваемых лиц, так как не имеет технической и юридической возможности их сопоставления*". Алена Попова подала заявление в ЕСПЧ, оспаривая законность технологии распознавания лиц.

Иными словами, официальная позиция московских властей, поддержанная судом, заключается в том, что ЕЦХД не обрабатывает, по крайней мере, биометрические персональные данные граждан и не идентифицирует лица на изображениях.

Согласно их объяснениям, при сравнении изображений людей, снятых в общественных местах, правительство Москвы использует технологию распознавания лиц только для сличения, а именно для поиска совпадения с изображением, предоставленным полицией, среди других изображений людей, хранящихся в ЕЦХД. Кроме того, следует отметить, что распознавание лиц осуществляется не в ЕЦХД, а в центральном хранилище всех изображений, полученных с видеокамер на улицах. Это ПАРСИВ (Подсистема автоматической регистрации сценариев индексирования видеоинформации), ИТ-решение, интегрированное с ЕЦХД города Москвы, осуществляет распознавание лиц и находит подходящие изображения. По своей сути ПАРСИВ — это шлюз, через который сотрудники полиции могут подключаться к городской системе

распознавания лиц для поиска подозреваемых в совершении преступлений.

После последнего обновления системы в 2021 году полицейские смогут применять множество фильтров для поиска человека: пол, возраст, раса, очки, борода, маска, головной убор и возможность распознавания силуэтов. ПАРСИВ позволяет отслеживать маршрут человека в заданном районе. Система находится в ведении правительства Москвы, а именно Департамента информационных технологий (ДИТ), который предоставляет доступ к ПАРСИВ различным ведомствам, в том числе и правоохранительным.

Мы полагаем, что, даже если и есть процедура и определенное регулирование рассматриваемой проблемы, она не подлежит ни общественному контролю, ни судебному надзору.

Отсутствие четкого регулирования использования системы распознавания лиц, ее допустимости в качестве судебного доказательства и общая непрозрачность соответствующих процедур способствуют злоупотреблению доступом полиции к базе данных и существованию черного рынка данных.

Первые признаки того, что общегородское распознавание лиц погрязнет в коррупции и злоупотреблению властью, появились в 2019 году. Тогда по меньшей мере 3 000 городских камер предоставляли изображения для системы распознавания лиц в рамках тестирования. Согласно результатам расследования журналиста Андрея Каганских, можно было купить дневной доступ к общественным видеокамерам (к прямому эфиру или к архивным записям) или отследить человека, найдя совпадения с предоставленным изображением.

В сентябре 2020 года Анна Кузнецова, волонтер “Роскомсвободы”, приобрела в интернете за 16 500 рублей (примерно 217,88 доллара США или 167,67 фунта стерлингов по среднему курсу Банка России на июнь 2020 года) pdf-файл с

изображениями с городских камер видеонаблюдения. Файл содержал в общей сложности 70 изображений ее лица с точностью 71 % и адреса, где они были сняты. Сотрудники Управления собственной безопасности МВД провели собственное расследование и подтвердили обвинения, используя тактику "контрольной закупки" с помощью двух волонтеров. В результате Следственный комитет России возбудил уголовное дело по фактам превышения должностных полномочий и нарушения неприкосновенности частной жизни (ст. 285 и ст. 137 УК РФ соответственно). Виновными оказались два сотрудника полиции. Один служил в Центре оперативно-розыскной информации Управления по СВАО ГУ МВД России по г. Москве и имел прямой доступ к ПАРСИВу. Другой — сотрудник ППС из местного отдела полиции, который выступал в качестве посредника между реальным исполнителем и лицами, заинтересованными в получении информации из баз данных. Согласно материалам судебного дела, публично обсуждавшимся в прессе, допрошенный в качестве свидетеля по делу начальник городского отдела видеонаблюдения ДИТ Дмитрий Головин заявил следователям, что силовики имеют право получать обезличенные авторизационные данные для доступа к ПАРСИВ. В СМИ сообщалось, что он добавил, что весь этот процесс подкреплен большим количеством соглашений, регламентов и поправок, в которых четко прописан порядок доступа к данным, а также указано, что разглашение этой информации третьим лицам строго запрещено. Однако нам не удалось найти ни одного обнародованного регламента или официального документа, подробно описывающего такое взаимодействие. Примечательно, что в СМИ также сообщалось, что Александр Кулик, руководитель отдела, где служили полицейские, являющийся свидетелем по делу, утверждал, что совершенно не знал о злоупотреблении полномочиями, а его подчиненный, вероятно, подглядел авторизационные данные Кулика во время работы с ПАРСИВом.

Первоначально суд первой инстанции принял крайне мягкое решение: оба виновных были оштрафованы на 20 000 и 10 000 рублей соответственно, а уголовное преследование в отношении них было прекращено за якобы имевшим место примирением сторон по ходатайству следователя. В итоге Московский городской суд, как апелляционная инстанция, отменил это решение и вернул дело на новое рассмотрение. Однако при повторном рассмотрении дела, суд вынес по существу такой же приговор. Тем не менее, это дело демонстрирует, что случайные изображения могут быть загружены и незаконно использованы без согласия субъекта, а персональные данные могут быть легко «слиты» и проданы

на черном рынке.

Еще одно дело, заслуживающее упоминания, связано с допустимостью результатов распознавания лиц в качестве доказательства в уголовном судопроизводстве. В феврале 2023 года Александр Цветков, 50-летний гидролог, был задержан сразу после прилета в аэропорту Домодедово и арестован по подозрению в нескольких убийствах, совершенных еще в 2002 году. Причиной ареста стало то, что его лицо после съемки на видеокамеру совпало с фотороботом убийцы, составленном по показаниям свидетелей, с вероятностью 55 %. Его обвинили в четырех убийствах и взяли под стражу. Несмотря на наличие алиби и показания многочисленных свидетелей в его пользу, он был освобожден из-под стражи только в декабре 2023 года, а обвинения в убийстве с него были сняты только в феврале 2024 года.

Это дело подняло вопрос о допустимости и достоверности использования результатов распознавания лиц в качестве доказательств в суде.

Суть проблемы заключается в отсутствии в законе определенного правила о том, какое минимальное значение точности результатов системы распознавания лица необходимо для его использования в качестве доказательства в судебном процессе.

Согласно анализу административных судебных процессов, проведенному опрошенным экспертом, не существует последовательных правил, выработанных судебной практикой.

Помимо распространения системы распознавания лиц в крупных городах, в конце 2022 года, когда вступил в силу закон о Единой биометрической системе, правительство стало единственным оператором биометрических персональных данных. Два типа биометрических персональных данных, а именно изображение лица и образец голоса, должны храниться исключительно в Единой

биометрической системе. Согласно ст. 15 Закона, обработка этих двух типов биометрических персональных данных вне ЕБС прямо запрещена. Все учреждения и организации должны были передать биометрические персональные данные, которые они ранее собирали в ходе своей деятельности. Более того, с принятием закона о Единой биометрической системе использование биометрии, а точнее, векторов, стало платной услугой, предоставляемой государством частным лицам и индивидуальным предпринимателям.

В целом части 15 и 16 статьи 3 Закона предусматривают такие механизмы обжалования, как право отозвать согласие на обработку биометрических данных, ограничить обработку или стереть биометрические данные и их векторы. С другой стороны, создание ЕБС само по себе является тенденцией к дальнейшей централизации обработки персональных данных, и правоохранительные органы получают доступ к системе ЕБС либо через отдельную IT-систему или ЕСИА (ч. 2 ст. 14), либо через прямой запрос информации, от которого оператор ЕБС не освобождается.

В настоящее время нет публичных свидетельств того, когда ЕБС использовалась в качестве самостоятельного инструмента наблюдения, однако мы предполагаем, что ЕБС — это лишь один из фрагментов общей архитектуры государственной слежки, дополняющий арсенал инструментов наблюдения, доступных правительству.

Мы предполагаем, что база данных ЕБС может быть использована в дальнейшем в качестве источника эталонных изображений для технологии распознавания лиц, поскольку сама ЕБС была разработана как центральная база данных, которую любой субъект или учреждение может использовать в качестве источника биометрических данных, а именно так называемых биометрических векторов, при условии заключения договора с оператором ЕБС. Более того, не существует никаких законодательных исключений, которые как-то ограничивали бы доступ правоохранительных органов. Напротив, законы, регулирующие такой

доступ, о которых мы упоминали в главе 1, достаточно широки по своему предметному охвату.

Единственным препятствием для использования ЕБС не как базы векторов, а как базы оригинальных биометрических данных является нехватка хранящихся в ней биометрических данных. Причина в том, что люди неохотно предоставляют свои биометрические персональные данные. Даже те, кто ранее давал согласие банковским учреждениям и чьи данные подлежат передаче в ЕБС, довольно часто прибегают к своему праву отказа, предусмотренному Законом о ЕБС.

> *В сентябре 2023 года Минцифры утверждало, что менее 1 % всего населения России отказалось от передачи своей биометрии в ЕБС. С другой стороны, Forbes сообщал, что после мошеннических звонков о невозможности отзыва согласия на передачу биометрии в будущем, число людей, обратившихся в местные центры госуслуг и решивших отказаться от передачи своих данных, выросло вдвое.*

Кроме того, мы хотели бы остановиться на будущих тенденциях, связанных с использованием системы распознавания лиц:

1. Дальнейшее развитие системы распознавания лиц в городе Москве.

   В недавно принятом бюджете города на 2024 год вдвое увеличены расходы на федеральную программу "Безопасный город", которая частично включает закупку видеокамер.

2. Развертывание аналогичных систем в других городах России и/или развитие тех, которые были установлены ранее, но не получили достаточного финансирования. В декабре 2023 года власти Санкт-Петербурга сообщили об установке около 20 000 "умных" камер, позволяющих использовать систему распознавания лиц. Кроме того, Министерство цифровых технологий предложило разработать общенациональную централизованную IT-платформу для хранения и

обработки данных видеонаблюдения. Наконец, Министерство транспорта отложило до 2025 года и последующих лет развертывание системы видеонаблюдения на транспорте, включая не только аэропорты, но и метро и другие виды общественного транспорта по всей стране.

3. Расширение системы распознавания лиц, ее развертывание в общественных зданиях, например, в государственных школах.

   В настоящее время как минимум в одной частной школе Московской области внедрено решение по распознаванию лиц, разработанное VisionLabs, филиалом Сбербанка. В 2021 году компания NtechLab, чьи решения поддерживают московскую систему распознавания лиц, провела тестирование системы распознавания лиц в школах разных регионов России. В 2013 году другой вендор, Inoface, резидент "Сколково", установил систему распознавания лиц в 7 государственных школах в нескольких городах Татарстана.

Несмотря на низкие стандарты качества изображений и отсутствие какого-либо парламентского либо судебного контроля, результаты распознавания лиц служат доказательством в суде, инструментом политических репрессий и продаются на черном рынке.

При этом, невзирая на множество рисков для прав человека (которые согласно новому европейскому закону об искусственном интеллекте отнесены к неприемлемым рискам), московские власти продолжают ежегодно рапортовать про десятки тысяч случаев поимки беглых преступников и невероятную динамику увеличения раскрытия преступлений. Однако результаты исследований независимых экспертов указывают на то, что распознавание лиц неэффективно в профилактике преступлений и поимке преступников. Судя по доступным данным, в Москве уровень раскрываемости тяжких и особо тяжких преступлений ниже среднего по стране (лидеры — Брянская и Тамбовская области, где систем распознавания нет). Исследование ИЦ “Коллективное действие” показывает небольшой рост в раскрываемости после 2020 года, но дефицит данных по преступности и вопросы к качеству ведения статистики не позволяют сделать однозначный вывод.

Теракт, произошедший в марте 2024 года в московском концертном зале “Крокус Сити Холл”, в результате которого погибли не менее 145 человек и еще 551 получили ранения, снова вернул российской общество к дискуссионному вопросу о необходимости и эффективности около 300 000 камер в столице с системой распознавания лиц, которые не помогли ни идентифицировать, ни помочь поймать до зубов вооруженных людей.

Распознавание лиц и международное право

В 2023 году ЕСПЧ в своем решении по делу «Глухин против России» единогласно постановил, что использование технологии распознавания лиц в режиме реального времени без применения соответствующих законодательно определенных процессуальных гарантий и механизмов надзора представляет собой нарушение права на частную жизнь, гарантированного статьей 8 Европейской конвенции по правам человека 1950 года.

Заявитель, Николай Сергеевич Глухин, гражданин России, 23 августа 2019 года проехал в московском метро с картонной фигурой в натуральную величину Константина Котова (участника акции протеста, дело которого вызвало общественный резонанс и привлекло широкое внимание СМИ), который держал в руках плакат с надписью: "Вы, наверное, шутите. Я Константин Котов. Мне грозит до пяти лет по [статье] 212.1 [УК РФ] за мирные протесты". В ходе мониторинга Интернета полиция обнаружила фотографии и видеозапись участия Глухина в демонстрации в метро, которые были выложены на одном из сайтов открытой социальной сети. Глухин подозревал, что против него может быть использована технология распознавания лиц, чтобы опознать его на скриншотах сайта социальных сетей и на записях с камер видеонаблюдения, установленных на станциях московского метрополитена, через которые он проходил 23 августа 2019 года. Спустя несколько дней он был задержан, предположительно для определения его местонахождения в метро в режиме реального времени была использована технология распознавания лиц.

Впоследствии Глухин был привлечен к ответственности по делу об административном правонарушении за то, что не уведомил власти о своем одиночном пикете с использованием "быстро (де)собираемого объекта". Он был оштрафован на 20 000 российских рублей (около 283 евро). Скриншоты сайта социальных сетей и видеозаписи с камер видеонаблюдения, через которые он

проходил 23 августа 2019 года, были представлены полицией в качестве доказательств против него.

30 октября 2019 года Московский городской суд оставил в силе его приговор в апелляционной инстанции, признав, в частности, что мирный характер демонстрации, в которой он участвовал, не имеет значения, а правонарушение было выявлено и доказательства собраны в соответствии с Законом о полиции. Однако суд также признал, что нарушение его права на частную жизнь само по себе, пусть и законное, имело место, о чем мы расскажем ниже.

ЕСПЧ отметил, что г-ну Глухину было сложно доказать свое утверждение о том, что в его деле была использована технология распознавания лиц. Анализируя вопрос о наличии и соразмерности вмешательства в право заявителя, ЕСПЧ указал, что законодательство государства-ответчика, в частности положения Закона о персональных данных, действовавшего на момент событий, а именно ч. 2 ст. 11, были сформулированы слишком широко и не содержали никаких ограничений в отношении характера ситуаций, в которых используются технологии распознавания лиц, прогнозируемых целей их использования, категорий людей, которые могут стать объектом распознавания, или ограничений в отношении обработки конфиденциальных персональных данных. Более того, государство не упомянуло ни о процессуальных гарантиях, ни о надзорном контроле, ни об имеющихся средствах правовой защиты, которыми будет сопровождаться использование технологии распознавания лиц в России. То есть национальное законодательство не предусматривало даже записи в официальных документах/базах данных или уведомления человека/общественности об использовании технологии распознавания лиц.

Тем не менее не было никакого другого объяснения тому, что полиция так быстро установила его личность после акции протеста. Государство также прямо не отрицало использование технологии распознавания лиц и не разъясняло, каким образом был опознан г-н Глухин. ЕСПЧ также принял к сведению имеющуюся в открытом доступе информацию о многочисленных случаях использования технологии распознавания лиц для идентификации участников акций протеста в России. Таким образом, ЕСПЧ пришел к выводу, что обработка персональных данных г-на Глухина в рамках возбужденного против него дела об административном правонарушении — в том числе использование технологии распознавания лиц для его идентификации и последующего установления его местонахождения и ареста — нарушила его право на уважение частной жизни.

С одной стороны, возможность такого вмешательства имело правовую основу в национальном законодательстве, предусмотренную Кодексом об административных правонарушениях и Федеральным законом "О полиции". Оба закона уполномочивают полицию расследовать административные правонарушения и собирать доказательства, в том числе доказательства, содержащие персональные данные. Иными словами, цель вмешательства в права г-на Глухина была законной — предотвратить административное правонарушение. С другой стороны, ЕСПЧ отметил отсутствие в национальном законодательстве подробных норм, регулирующих объем и применение мер, связанных с использованием технологии распознавания лиц, а также отсутствие надежных гарантий против риска злоупотреблений и произвола. Меры, предпринятые в отношении г-на Глухина, были особенно неадекватными с учетом того, что это это была мирная акция протеста, которая не представляла никакой опасности для общества или безопасности транспорта. Фактически она привела лишь к его привлечению к ответственности за незначительное правонарушение. Таким образом, обработка биометрических персональных данных заявителя с использованием технологии распознавания лиц в рамках производства по делу об административном правонарушении — во-первых, для установления его личности по фотографиям и видео, опубликованным в Интернете, и, во-вторых, для его обнаружения и задержания во время поездки в московском метро — не соответствовала "настоятельной общественной потребности" и не могла рассматриваться как "необходимая в демократическом обществе".

ЕСПЧ счел меры, принятые в отношении заявителя, "особенно интрузивными", поскольку они касались технологии распознавания лиц в режиме реального времени. Обработанные персональные данные содержали информацию об участии заявителя в мирном протесте, а значит, раскрывали его политические взгляды. Соответственно, они относились к специальной категориям конфиденциальных данных, требующих повышенного уровня защиты. Суд также указал, что использование такой особо инвазивной технологии для выявления и ареста участников мирных протестов может негативно сказаться на правах на свободу выражения мнения и собраний.

В этих обстоятельствах Суд пришел к выводу, что использование технологии распознавания лиц для идентификации заявителя не отвечает "настоятельной общественной потребности" и несовместимо с идеалами и ценностями

демократического общества, основанного на верховенстве права, которые призвана поощрять и поддерживать Европейская конвенция.

Послесловие. Теневая слежка в России, деанон, профайлинг и хакинг

В этой части нашего исследования мы хотели бы обсудить вопросы, которые заслуживают дальнейшего изучения. Однако главная проблема заключается в том, что использование профайлинга и хакинга не поддается всестороннему анализу. Причиной тому является отсутствие специализированных нормативных актов и официальных документов, подробно описывающих эти две практики. Более того, вокруг них существует множество устных сообщений и эпизодических случаев, но публично доступных доказательств очень мало. В основном о них сообщают инсайдеры и эксперты. Здесь мы приводим информацию, полученную от этих экспертов.

Профайлинг

Профилирование существует в некоторых аспектах официальной правоохранительной деятельности, а именно в рамках оперативно-розыскных мероприятий. Так называемое дело оперативного учета — засекреченное дело, открытое и ведущееся соответствующими правоохранительными органами, уполномоченными осуществлять оперативно-розыскную деятельность — подпадает под общее понимание профайлинга. Однако один из опрошенных экспертов обратил наше внимание на черный рынок данных и некоторые скрытые методы работы информационных

посредников. Современный ландшафт профайлинга можно кратко описать как состоящий из следующих участников.

Различные программные решения, разработанные специально для информационной аналитики или OSINT, например, Medialogia, программное решение, предназначенное для мониторинга социальных сетей и онлайн-СМИ, может быть использовано в качестве инструмента для профилирования онлайн-активности интернет-пользователей.

Разработчик, Автономная некоммерческая организация "Диалог" (АНО "Диалог"), общероссийский государственный межведомственный центр компетенции в области интернет-коммуникаций и оператор цифрового диалога власти и общества, помогает местным властям отслеживать социальную активность и оказывает им PR-услуги. Другой пример — Social Data Hub, ранее предоставлявший свои услуги как частным структурам (например, банкам), так и государству по сбору информации из социальных сетей и профилей приложений.

Также известно о государственных IT-решениях, например, Oculus и "Вепрь", разработанных подведомственной Роскомнадзору структурой — Главным радиочастотным центром (ГРЧЦ). Согласно официальным пояснениям, первый предназначен "для поиска запрещенного контента и выявления нарушений [соответствующего] законодательства в изображениях и видеоматериалах". В задачи второго входит "обнаружение потенциальных точек напряженности в сети, способных перерасти в информационные угрозы". Опрошенный эксперт пояснил, что последняя отвечает за мониторинг наиболее активных граждан в Сети. Примечательно, что Роскомнадзор ведет профилирование против политических и общественных активистов. Благодаря утечке данных из ГРЧЦ (известная как #RussianCensorFiles), стало известно, например, о существовании списка из более чем 800 человек, которые могут быть объявлены иностранными агентами, и только 139 человек были объявлены тогда иностранными агентами.

Существуют нерегулируемые программы-парсеры, которые извлекают из сети информацию, зачастую защищенную законом, и впоследствии распространяют ее через телеграм-ботов. Самым известным примером был и, вполне возможно, остается “Глаз Бога”. Он был популярен даже среди полицейских из разных отделов и подразделений, поскольку был гораздо удобнее их систем и не требовал никакой административной волокиты. Более того, как нам сообщил источник, разработчики подобных онлайн-сервисов довольно часто предоставляют эксклюзивный доступ для сотрудников правоохранительных органов.

Еще в 2020 году МВД предложило рассмотреть возможность создания мобильного приложения, установка которого будет обязательной для всех рабочих мигрантов, прибывающих в Россию. Данное предложение включено в прогноз развития миграционной обстановки, составленный экспертами ведомства. В рамках эксперимента МВД предложило рассмотреть разработку и формирование цифрового профиля мигранта, отражающего так называемый "рейтинг социального доверия", в котором должна содержаться полная информация о социально-правовом положении мигранта, биометрические данные, сведения о здоровье, уголовное прошлое или его отсутствие. Идея такого профиля содержится в Концепции миграционной политики, которую правительство утвердило в январе 2024 года.

После теракта в «Крокус Сити Холле» 22 марта 2024 года к идее вернулись. Вице-спикер Госдумы Сергей Неверов заявил о том, что решение создание такого профиля согласовано с премьер-министром, а система будет внедрена до конца 2024 года. С помощью цифрового профиля МВД сможет установить, куда мигрант перемещается, где и с кем проживает, когда у него истекает срок действия разрешительных документов, на какую работу он устраивается и с какой увольняется.

Деанонимизация

Для того чтобы иметь возможность идентифицировать пользователей интернета и наказывать их за слова, государство ставит своей целью провести цифровую паспортизацию российского общества и поголовную деанонимизацию пользователей сети. Эти цели не скрываются.

Так, согласно Стратегии развития информационного общества до 2030 года, утвержденной Указом Президента РФ (подп. “д”, п. 34), для обеспечения функционирования социальных, экономических и управленческих систем с использованием российского сегмента сети Интернет российским властям необходимо создать новые механизмы партнерства стейкхолдеров и систему доверия, исключающую анонимность, безответственность и безнаказанность правонарушителей в сети Интернет.

Как видно, анонимность перечислена через запятую
с безнаказанностью и безответностью
и рассматривается как “баг Интернета”,
а не его “фича”.

В марте 2023 года в результате журналистского расследования стало известно, что «Ростех» научился вычислять владельцев анонимных телеграм-каналов и собирается продавать эту услугу МВД и ФСБ России. Программный комплекс под наименованием «Охотник», по заявлениям разработчиков, способен устанавливать аккаунты администраторов и владельцев телеграм-каналов с помощью собственной нейросети. Личности администраторов каналов идентифицируют по номеру мобильного телефона, данным геолокации и IP-адресу. Помимо этого, если верить техническому описанию программы, «Охотник» исследует и различные источники открытых данных: социальные сети, блоги, форумы, мессенджеры, доски объявлений,

блокчейны криптовалют, ресурсы даркнета и государственные автоматизированные сервисы.

Через год последовало еще одно расследование журналиста Андрея Захарова, после которого также стало известно, что МВД трех регионов РФ уже закупили систему «Инсайдер» как часть программного обеспечения “Демон Лапласа” для слежки за группами, аккаунтами и чатами в VK и деанонимизации пользователей Telegram.

Взломы

Что касается взлома, то правовые основания для такой практики установлены Законом "Об оперативно-розыскной деятельности" (подробнее см. главу 1). Опрошенный эксперт отметил, что нередко оперативники сами не получают доступ к устройству интересующего их лица после его изъятия в ходе следственных действий, а прибегают к помощи "черных хакеров", которые сотрудничают, как правило, под принуждением, в обмен на попустительство их преступлениям.

Однако в открытом доступе нет достоверной информации об успешном удаленном доступе к устройствам пользователей. Причина популярности такой практики, как изъятие телефонов в целях взлома кроется в том, что о ней официально не сообщается. По словам эксперта, точные инструменты, используемые в настоящее время, неизвестны, но он упомянул, что некоторое время назад Elcomsoft и Cellebrite закупались и якобы использовались правительством. В 2021 году Cellebrite заявила о прекращении продаж своих решений в РФ.

И несмотря на инцидент с Галиной Тимченко, издателем и соучредителем российского независимого СМИ Meduza, чей телефон был заражен шпионской программой Pegasus, до сих пор неизвестно, кто стоит за атакой. Также в настоящее время нет никакой информации о продаже установок Pegasus в Россию компанией NSO Group.

В заключение мы считаем, что эти два аспекта — профилирование и взломы — заслуживают дальнейшего изучения с упором на поиск и проверку фактов. Такие исследования могут способствовать лучшему пониманию реалий использования профайлинга и социального мониторинга, а также угроз, связанных с использованием хакерских атак против активистов, бизнесменов и политиков.

Заключительные аргументы

Подводя итог, можно сказать, что российское государственное наблюдение имеет следующие характеристики:

- направлено на неизбирательную слежку за гражданами, а также иностранцами, в т.ч. за трудовыми мигрантами;
- существует в условиях продолжающихся попыток паспортизации каждого пользователя Интернета и деанонимизации пользователей социальных сетей, в том числе с применением технологических решений;
- используется неподотчетное наблюдение за интернет-коммуникациями, которое нарушает принцип соразмерности, поскольку конкретные подходы или критерии засекречены и наблюдение может использоваться без разбора;
- отсутствуют эффективные средства правовой защиты для тех, чье право на частную жизнь было нарушено государственными служащими;
- опирается на техническую инфраструктуру, интегрированную в сети, и провайдеров услуг как агентов государственного наблюдения, что позволяет осуществлять массовую слежку за пользователями;
- отсутствует правовое регулирование использования биометрических персональных данных в целях наблюдения, что размывает границы между онлайн- и офлайн-наблюдением и делает систему неподотчетной, подверженной злоупотреблениям и коррупции;

- законодатели постоянно используют открытые цели и соответствующие формулировки при разработке законопроектов, обеспечивая тем самым широкую свободу действий для правоприменителей, что, как следствие, приводит к злоупотреблению властью;
- прослеживается явная стратегия правительства маскировать использование технологии распознавания лиц и применение других спорных практик крайне расплывчатыми формулировками, а также прятать данные об использовании с помощью ограничения доступа к внутренним документам и распространение на них режимов конфиденциальности и другим мерам защиты.

Команда

RKS Global

info@rks.global ▪ rks.global