Пандемия слежки

Глобальный кризис здравоохранения, вызванный пандемией новой коронавирусной инфекции, стал предлогом для серьезного расширения слежки за людьми в значительной части мира. Наиболее уязвимыми оказались граждане авторитарных государств. Введение карантина послужило катализатором развития всех видов слежения, однако, прежде всего – цифровых технологий. Единственным ограничением оказались финансовые возможности региональных властей, которым и делегировали основные полномочия по борьбе с пандемией. Богатые регионы получили карт-бланш на полный контроль передвижения жителей любыми доступными способами.

Мы насчитали шесть отдельных технологий сбора и проверки сведений о частной жизни граждан, которые в совокупности погружают нас в «прекрасный новый мир» тотального слежения: централизованный сбор информации о гражданах, прибывающих в страну, регион или населенный пункт; система цифровых или аналоговых пропусков, позволяющих ограничивать виды транспорта и цели передвижения, а также дифференцировать граждан по объему прав; видеонаблюдение, в том числе с функцией распознавания лиц; отслеживание местонахождения граждан по геолокационным данным, передаваемым мобильными устройствами и следящими приложениями; расширение

возможностей слежки путем делегирования полицейских функций частным субъектам и представителям иных ведомств.

В будущем, при «чрезвычайных» обстоятельствах, которыми отныне может быть объявлено все, что угодно – от новой эпидемии или техногенной катастрофы до массовых акций протеста – накопленный во время карантина опыт и ресурсы позволят быстро развернуть плотное наблюдение и дифференцировать граждан по объему прав и свобод. Более того – как оказалось, для этого властям даже не требуется объявлять чрезвычайную ситуацию или чрезвычайное положение.

Никаких законов, регулирующих пределы вмешательства в частную жизнь с помощью электронных технологий, в России, по сути, нет. Существующие положения Конституции и общие нормы отраслевого законодательства обесцениваются правоприменительной практикой и абсолютной поддержкой, которую российские суды готовы оказывать исполнительной власти и силовым органам.

Кроме того, выяснилось, что некоторые регионы и ведомства намерены сохранить ряд опробованных технологий и в «мирное» время. Так, власти Белгородской области по собственной инициативе попросили включить регион в эксперимент по использованию приложения для слежки от Минкомсвязи, ссылаясь на необходимость подготовиться к будущим чрезвычайным ситуациям.

СМИ также сообщали, что МВД рассматривает вопрос об использовании следящих приложений и внедрении «рейтинга социального доверия» для всех въезжающих в страну мигрантов.

Можно предположить, что приложения для отслеживания геолокации будут использоваться в качестве средства контроля соблюдения ограничительных мер – вроде домашнего ареста, административного надзора и т.п.

Развитие коронавирусной слежки повлекло за собой расширение применения и других, не связанных с ней напрямую технологий и практик. К примеру, МВД, ФСБ и Минкомсвязь уже подготовили законопроект, распространяющий обязанность операторов связи в течение трех лет хранить информацию о фактах приема, передачи, доставки и обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- и любых иных сообщений на всех владельцев технологических сетей связи и точек обмена трафиком.

Большой московский брат

В отличие от подавляющего большинства российских регионов, которые ограничились отдельными мероприятиями, Москва взяла от карантина максимум, организовав широкомасштабное тестирование различных технологий цифрового и «аналогового» контроля за гражданами. Если раньше мониторингу подвергались отдельные «неблагонадежные» категории (экстремисты, гражданские активисты, футбольные фанаты, правозащитники, члены неформальных объединений и субкультурных групп), то сейчас – обычные граждане, которых разделили на категории, дифференцированные по объему прав и возможностей.

По сути, пандемия-2020 стала вторым после Чемпионата мира по футболу-2018 поводом создать и проверить в боевых условиях технологию именно массовой слежки. Строго говоря, у Москвы было для этого гораздо больше возможностей и оправданий: с одной стороны столица – одна из лидеров цифрового развития, с другой – крупнейший очаг инфекции в стране.

К 2020 году в Москве создана крупнейшая в России сеть камер уличного и подъездного видеонаблюдения, подключенная к системе распознавания лиц. По данным городского Департамента информационных технологий, сеть включает в себя более 178 тыс. камер, установленных в 102 тыс. подъездов и 21 тыс. дворов, не считая видеонаблюдения в государственных и муниципальных учреждениях и прочих общественных местах. Эта сеть использовалась для выявления нарушителей карантина.

Московские власти одними из первых объявили о введении цифровых пропусков и смогли быстро запустить эту систему на базе портала городских услуг. Система отслеживала данные транспортных карт и номера личных автомобилей, а сеть дорожных камер использовалась для фиксации нарушений и массового оформления штрафов за езду по городу без пропуска.

Фактически в Москве мы наблюдаем наиболее разветвленную систему массовой слежки в сочетании с дифференциацией граждан по объему доступных прав и свобод. Всех жителей столицы можно условно разделить на 4 категории.

Привилегированные. Им не обязательно соблюдать самоизоляцию, позволено покидать место жительства, в том числе ходить на работу, они не подлежат электронному мониторингу и могут не оформлять цифровые пропуска. В эту группу входят сотрудники организаций и

органов власти, чье нахождение на рабочем месте является критически важным для обеспечения их функционирования, работники здравоохранения, а также иные граждане, определенные решением Штаба; сотрудники правоохранительных органов, МЧС и Роспотребнадзора; волонтеры, таксисты, строители и сотрудники предприятий по обслуживанию инфраструктуры и жизнеобеспечению; военнослужащие, государственные и муниципальные служащие и лица, замещающие государственные и муниципальные должности, судьи, адвокаты, нотариусы, включая помощников, журналисты, частные охранники.

Обычные. Все граждане, не относящиеся к другим категориям, которые обязаны соблюдать режим самоизоляции, а при выходе из дома оформлять цифровые пропуска, количество и продолжительность действия которых ограничены.

Пораженные в правах. Лица, прибывшие из опасных территорий, а также проживающие с ними совместно, лица старше 65 лет, а также те граждане, которые имеют заболевания из списка, утвержденного властями. Они обязаны соблюдать изоляцию, не имеют права покидать место жительства без особых оснований, для чего требуется оформление цифрового пропуска.

Изолированные. Лица с диагностированным COVID-19 или ОРВИ, а также проживающие с ними лица (по индивидуальному постановлению). Им нельзя покидать место жительства, они подлежат обязательному электронному контролю с помощью следящего приложения «Социальный мониторинг».

Общероссийские мероприятия

С начала марта 2020 года главный санитарный врач России издал серию приказов в целях снижения рисков завоза и распространения новой коронавирусной инфекции, согласно которым главы российских регионов обязаны обеспечить изоляцию всех прибывающих из-за границы граждан в течение 14 дней со дня прибытия, а также организовать контроль за соблюдением режима изоляции и работу горячей линии для сбора информации о гражданах.

Региональные власти, в свою очередь, передавали контрольные полномочия на муниципальный уровень. К примеру, губернатор Астраханской области Игорь Бабушкин на встрече с главами районов прямо заявлял: «Все граждане, кому необходима самоизоляция при

коронавирусе, должны быть на контроле сотрудников внутренних дел. И вы также обязаны о них всё знать».

Кроме того, каждый прибывший в страну обязывался незамедлительно сообщать о своем возвращении в Российскую Федерацию, предоставляя довольно много личной информации — место и даты пребывания за рубежом, а также сведения о регистрации и месте фактического жительства.

Часть регионов начала вводить подобные ограничения раньше, однако и информации они зачастую собирали меньше. К примеру, москвичей обязали сообщать о прибытии из стран и территорий, в которых зарегистрированы случаи новой коронавирусной инфекции, еще 5 марта, но — кроме контактной информации — ничего не требовали. В Санкт-Петербурге, Новгородской области и ряде других регионов обращение на горячую линию Роспотребнадзора первоначально вообще носило рекомендательный характер.

При этом власти явно давали понять гражданам, что в любом случае знают, кто и когда пересек государственную границу, напоминая об административной и уголовной ответственности за несоблюдение режима изоляции, за которым следит полиция при поддержке ФСБ, народных дружинников, квазиобщественных объединений, казаков, спасателей и прочих привлеченных субъектов. Известны случаи, когда гражданам, прибывшим из-за рубежа, которых не опрашивали на границе и которые не сообщали о себе на горячую линию, тем не менее звонили из поликлиники по месту жительства с вопросами о самочувствии и напоминанием о необходимости соблюдать самоизоляцию.

В отношении прибывающих из-за границы и выявленных больных коронавирусной инфекцией сотрудники Роспотребнадзора в массовом порядке проводили эпидемиологическое расследование, в том числе проводили анкетирование в аэропортах и на железнодорожных вокзалах: запрашивали данные о месте жительства, контактных телефонах и т.п. Медицинские работники, приходившие по месту жительства, собирали информацию о совместно проживающих, соседях, сослуживцах, близких родственниках. Возможность проведения санитарно-эпидемиологических расследований предусмотрена ст.42 Федерального закона «О санитарно-эпидемиологическом благополучии населения», однако специальное законодательство не дает Роспотребнадзору полномочий по сбору и

обработке сведений о частной жизни граждан и вообще не определяет пределы вторжения в частную жизнь.

Впоследствии требование уведомлять о своем прибытии в ряде регионов распространили на всех пересекающих административную границу субъекта Федерации. В Мурманской области обязали сообщать о месте, датах пребывания на территориях других регионов, контактную информацию, в том числе об адресе нахождения на самоизоляции.

Региональные горячие линии стали первым звеном в цепочке сбора сведений о гражданах под предлогом борьбы с эпидемией. Следующий уровень – обработка и обмен информацией.

31 марта правительство утвердило Временные правила учета информации в целях предотвращения распространения новой коронавирусной инфекции, закрепившие централизованную систему обмена данными. Согласно этому документу, а также методическим рекомендациям Минздрава, при сборе данных эпидемиологического анамнеза устанавливается наличие зарубежных поездок за 14 дней до первых симптомов, а также наличие тесных контактов за последние 14 дней с лицами, подозрительными на инфицирование, или теми, у которых диагноз подтвержден лабораторно.

В централизованную базу данных включаются следующие сведения о лицах с подтвержденным диагнозом новой коронавирусной инфекции, госпитализированных с симптомами пневмонии, а также всех контактировавших с указанными группами: фамилия, имя, отчество, дата рождения, пол, гражданство, адрес регистрации и фактического места жительства, абонентский номер сотовой связи.

У инфицированных COVID-19 и госпитализированных с пневмонией дополнительно запрашивают широкий круг медицинской и эпидемиологической информации: сведения о медицинском страховании, сведения об обследованиях и проводивших их медицинских организациях, о беременности и вакцинации, сопутствующие диагнозы, о передвижениях[1], в том числе по территории России (документ, по которому приобретался билет, пункты отправления и назначения, маршрут следования и т.п.). Кроме того, по решению оперативного штаба база может быть дополнена любыми

[1] Отметим, что согласно правилам пассажирских перевозок (авиационным, железнодорожным и междугородним автобусным транспортом), при приобретении билетов необходимо предъявлять паспорт, а данные пассажира регистрируются в централизованных базах данных, доступных сотрудникам полиции. В сочетании с системой «Сторожевой контроль» это позволяет отслеживать перемещения любых интересующих власти лиц общественным транспортом.

иными сведениями, которые штаб сочтет нужными. Оператором базы является министерство здравоохранения, а доступ к ней имеют подведомственные Минздраву федеральные учреждения, Росздравнадзор, МВД, Роспотребнадзор, Федеральное медико-биологическое агентство, некие «поставщики информации», а также «иные органы и (или) организации по решению оперативного штаба». Подобные решения не публикуются и не объясняются.

Дополнительно министерство связи получает от сотовых операторов сведения о передвижении человека по стране на основе данных биллинга и передает их в централизованную базу данных. Эта система должна использоваться в том числе для отслеживания контактов больных и инфицированных, а также для рассылки оповещений о необходимости самоизоляции.

На практике некоторые пользователи в Красноярском и Краснодарском краях получали от абонента «MCHS» sms-сообщения следующего содержания: «Убедительная просьба вернуться домой! Воздержитесь от прогулок! Находясь на улице, вы подвергаете свою жизнь и жизнь других людей опасности! Выход из дома без крайней необходимости запрещен!». ПАО «Вымпелком» отказалось предоставить информацию о пределах и основаниях отслеживания геолокационных данных абонентов, а МЧС и ООО «Скартел» проигнорировали адвокатский запрос.

В Татарстане на первой версии портала оформления sms-пропусков имелось предупреждение: «Если вы в течение дня будете систематически отдаляться от дома — система это увидит и будут приняты меры». Поскольку устанавливать специальное программное обеспечение на мобильные устройства не требовалось, отслеживать перемещения, вероятно, предполагалось на основании данных сотовых операторов. Позднее это предупреждение удалили с сайта.

В начале июля Минкомсвязь опубликовала проект регламента обмена информацией о местонахождении граждан, контактировавших с больными COVID-19, определяемом на основании данных сотовых операторов. Согласно документу, Минкомсвязи будет ежесуточно получать от операторов информацию обо всех следующих абонентах:

— находящихся за рубежом;

— пересекших границу Российской Федерации (по ним будет отслеживаться соблюдение режима самоизоляции и перемещение за пределы зоны самоизоляции (от 500 до 2000 метров) в течение 14 суток

после пересечения государственной границы на основании данных о геолокации абонента в течение первой ночи).

— возможно контактировавших с заболевшими абонентами (на основании данных геолокации, сведений о звонках и sms).

Доступ к системе будут иметь Минкомсвязи, Минздрав, МВД, Росгвардия, органы исполнительной власти и региональные штабы.

Сбор информации непосредственно от граждан, а также централизованная обработка геолокационных данных — единственные мероприятия, которые проводили в масштабах всей страны. В остальном у региональных властей была возможность выбора стратегии и методов слежки, которыми они пользовались в разной степени.

«Аналоговые» и цифровые пропуска

Власти 23 российских регионов, а также в Севастополе в той или иной форме ввели так называемые «цифровые пропуска» — буквенно-цифровые коды, получение которых необходимо для выхода из дома в условиях карантина либо для передвижения на личном и/или общественном транспорте. В 15 регионах, а также Крыму ввели «аналоговые» пропуска (оформляемые, как правило, работодателями для сотрудников, которым разрешено продолжать работу не в дистанционной форме) в качестве самостоятельной или дополнительной меры. Кроме того, 19 регионов объявили о принципиальной готовности ввести цифровые пропуска в случае ухудшения эпидемиологической обстановки или в будущем при возникновении чрезвычайной ситуации.

Системы для оформления цифровых пропусков создавались в экстренном порядке без независимого аудита, что не могло не сказаться на качестве и безопасности. К примеру, вскоре после релиза соответствующего приложения в Москве эксперты выявили целый ряд уязвимостей — приложение получает доступ ко всем данным и настройкам, включая установление соединения с устройствами Bluetooth, GPS, камеру и звонки, отключение спящего режима, просмотр сетевых подключений; приложение передаёт собранную информацию в открытом виде без какого-либо шифрования; для распознавания лиц приложение использует эстонский сервис identix.one, передавая данные через серверы, расположенные за пределами Российской

Федерации; в QR-кодах, генерируемых приложением, зашифрованы MAC и IMEI (индивидуальные идентификаторы) устройства.

При оформлении цифрового пропуска в Москве требовалось дать Департаменту предпринимательства, Департаменту информационных технологий и ряду других подведомственных московским властям учреждений разрешение на обработку передаваемых персональных данных, включая их передачу третьим лицами и рассылку рекламных сообщений сроком на десять лет.

Делегирование полицейских функций

Власти почти половины российских регионов предоставили чрезвычайные полномочия, включающие возможность вмешиваться в частную жизнь граждан, крайне широкому кругу субъектов — от медицинских работников и спасателей до таксистов, народных дружинников и членов казачьих обществ. Это привело в том числе к применению явно незаконных дискриминационных практик в отношении представителей уязвимых групп.

Одна из основных противоэпидемических мер в России — изоляция граждан и ограничение передвижений как между субъектами Федерации, так и внутри населенных пунктов. Ограничения зависят как от цели, так и от способа передвижения, а за нарушения предусмотрены санкции.

С 1 апреля федеральный Кодекс об административных правонарушениях дополнили нормами об ответственности за невыполнение противоэпидемических мероприятий в период чрезвычайной ситуации, карантина или угрозы распространения опасных заболеваний (ч.2 ст.6.3), а также невыполнение правил поведения при режиме повышенной готовности (ст.20.6.1). Подобные нормы появились также в законодательстве об административной ответственности некоторых субъектов.

После введения в российских регионах режима повышенной готовности территориальные управления МВД получили предписание оказывать исполнительным органам власти содействие в реализации мер по противодействию распространению новой коронавирусной инфекции.

По мере того, как в ряде регионов вводили карантин и требования изоляции граждан, прибывающих из других субъектов Федерации,

муниципалитетам, в свою очередь, поручили организовать сбор и предоставление в МВД информации о таких лицах.

Главной задачей стало выявление прибывающих в регион граждан, а также создание условий для контроля изоляции (в том числе — фотографирование, анкетирование, сбор сведений о фактическом месте жительства и пребывания) и проверка соблюдения карантинных мероприятий (основания нахождения вне места жительства, наличие пропуска).

Как минимум в 38 российских регионах, а также на территории Крымского полуострова власти привлекали к контрольным мероприятиям посторонних лиц — членов ветеранских и «военно-патриотических» организаций, народных дружинников, представителей «местного актива», курсантов, чиновников муниципалитетов, представителей «Общероссийского народного фронта» [2] , работников муниципальных учреждений и социальных организаций из сфер культуры, спорта и образования, сотрудников пожарно-спасательного центра, спортсменов.

Как правило, они патрулировали улицы совместно с сотрудниками полиции, ограничиваясь объяснением гражданам необходимости социального дистанцирования и изоляции, однако известны случаи более серьезного ограничения приватности.

Так, власти Краснодара отчитывались о создании «мобильных отрядов самоконтроля для патрулирования улиц и территорий общего пользования», которые «тех, кто нарушает карантин и без причины находится на улице, отправляют домой; к тем, кто отказывается идти домой, применяются меры административного и уголовного порядка».

В Приморском крае власти предложили частной компании осуществлять контроль территории с помощью промышленных дронов, оснащенных тепловизорами.

Помимо проверки документов, казачьи патрули как минимум в Рязанской и Свердловской областях осуществляли этнический профайлинг. В интервью государственному новостному агентству представитель казачьего общества утверждал, что патрули «смотрят на людей "китайской принадлежности" и на всех, кто чихает, обращают внимание, предлагают пройти в поликлинику в сопровождении патруля, но в добровольном порядке». Отметим, что этнический

[2] Созданное в 2011 году по инициативе Владимира Путина квазиобщественное объединение.

профайлинг (этническое профилирование) признан одной из форм дискриминации, запрещенной международным правом.

Законом подобные функции (за исключением явно незаконных действий) в порядке изъятия из общего правила неприкосновенности частной жизни и свободы передвижения возложены на полицию и Росгвардию. Карантин вынудил власти значительно (до неопределенного) расширить круг лиц, которым позволено опрашивать граждан, контролировать их и ограничивать свободу передвижения, наделив их неясными полномочиями.

Помимо сбора эпидемиологического анамнеза, в некоторых регионах, использующих для контроля соблюдения карантина системы видеонаблюдения и распознавания лиц, медицинским работникам предписывалось передавать сведения о пациентах, включая фамилию, имя, отчество, диагноз и иные медицинские сведения в централизованные базы данных, а также фотографировать их — тоже явно не свойственные врачам чрезвычайные полномочия.

При этом, если передача сведений, составляющих врачебную тайну, без согласия пациента возможна при угрозе распространения инфекционных заболеваний в силу п.2 ч.4 ст.13 Федерального закона «Об основах охраны здоровья граждан в Российской Федерации», то фотографирование регламентировано лишь ведомственными инструкциями, не гарантирующими соблюдение прав. В частности, в Москве обязанность фотографировать пациентов возложили на сотрудников бригад скорой медицинской помощи, которых для этих целей специально снабдили электронными устройствами.

Распознавание лиц

Российские власти начали массово внедрять системы публичного видеонаблюдения и распознавания лиц в преддверии Чемпионата мира по футболу FIFA. Так, с 2015 года во всех российских регионах внедряется аппаратно-программный комплекс «Безопасный город». В его основе лежит план построения разветвленной системы видеонаблюдения и видеофиксации с возможностью автоматизированного обмена информацией, анализа видеопотока, распознавания и идентификации лиц, а также позиционирования движущихся объектов.

Осенью 2017 года мэрия Москвы впервые сообщила о запуске системы массового распознавания лиц. На тот момент сообщалось, что к ней подключили более трех тысяч видеокамер, изображение с которых автоматически анализируется в режиме реального времени. При помощи нейросетей лица попавших в камеру прохожих сравнивают с фото из баз данных.

Вся информация с камер наблюдения передается в Единый центр хранения и обработки данных (ЕЦХД). К нему предоставляется доступ представителям правоохранительных органов и органов исполнительной власти с рабочих мест. Анализ московского законодательства, проведенный юристами Международной Агоры, свидетельствует, что основания, принципы, правила и порядок использования технологии распознавания лиц не были сформулированы должны образом. В частности, не определены:

— допустимые случаи и цели применения технологии;

— порядок использования технологии уполномоченными органами власти (длительность применения технологии, срок хранения полученных биометрических данных, способы обработки и т.д.);

— механизмы защиты прав и интересов субъектов персональных данных при применении технологии.

На это обращали внимание гражданская активистка Алена Попова и политик Владимир Милов, оспаривая использование распознавания лиц против участников протестных митингов в Москве. В ответ представители Департамента информационных технологий утверждали, что существующего регулирования достаточно, а технология не нарушает прав граждан.

В середине марта московские власти отчитались о выявлении 200 нарушителей карантина с помощью системы «Безопасный город». При этом известно как минимум об одном случае вероятно ложного срабатывания системы в Южно-Сахалинске.

В настоящее время системы видеонаблюдения с распознаванием лиц установлены в большинстве крупных городов страны. Как минимум в 11 регионах, а также в Крыму эти системы использовали для выявления нарушителей карантина.

Власти Сахалинской, Астраханской и Белгородской областей, а также Москвы и Санкт-Петербурга во время карантинных ограничений продолжали закупать дополнительные системы слежки, в том числе видеонаблюдения и обработки биометрических данных.

При этом доступ к системам видеонаблюдения, вероятно, можно купить на «черном» рынке. Судя по всему, ничего принципиально не изменилось с декабря 2019 года, когда журналист Андрей Каганский провел «контрольную закупку» собственной выписки из базы московского ЕЦХД. Уже в июле 2020 года в Сети появилось объявление о продаже доступа к система московского видеонаблюдения, включая архив данных.

Разглашение диагнозов и утечки личных данных

Как минимум в 18 регионах сообщалось об утечках чувствительной информации, собираемой властями в рамках борьбы с эпидемией, включая диагноз и другие медицинские сведения, адреса, номера телефонов и т.п. Чаще всего личные данные публиковались в виде списков инфицированных или контактировавших лиц либо сообщений о диагнозе отдельных пациентов.

В Чувашии в мессенджерах распространяли список 17 жителей республики с подтвержденным диагнозом COVID-19 — опубликованы фамилии, возраст, адреса и места работы.

В Брянской области в социальной сети появилась справка о заболевших супругах, которая включала не только сведения о пациентах, но и их родственниках — фамилии, адреса и место работы.

В Курганской области прибывшая из Москвы женщина подверглась травле после того, как в городском паблике выложили результаты ее анализа.

В Воронежской области в Сеть попал официальный документ Роспотребнадзора, направленный в адрес Россошанской районной больницы и содержавший сведения о диагнозе, домашнем адресе и контактных лицах женщины, скончавшейся от коронавирусной инфекции.

В Иркутской области рассылались сообщения с именами (включая имена несовершеннолетних детей), адресом и местом работы семьи, вернувшейся из отпуска. По словам женщины, информацию опубликовали спустя всего полчаса после того, как им сообщили результаты анализов.

Интернет-издание Mash опубликовало онлайн-карту Москвы и Московской области, на которой были обозначены дома, у жильцов которых диагностирован COVID-19. Источником информации на карте

указаны «Федеральный и региональные оперштабы по борьбе с вирусом». Подобную карту в течение некоторого времени публиковали власти Тульской области, закрывшие проект после жалоб жителей.

Уязвимость системы онлайн-оплаты штрафов в Москве позволила получить доступ к паспортным данным оштрафованных по уникальному номеру начисления (УИН), который можно подобрать помощью программы.

Предположительная утечка в Оренбургской области, возможно, продемонстрировала методы работы МВД, на которое де-факто возложили обязанность контролировать соблюдение изоляции и отслеживать перемещения лиц, которым поставлен диагноз COVID-19, а также контактировавших с ними лиц. Так, в мессенджерах распространяли документ, озаглавленный «Список лиц, поставленных на сторожевой контроль как возможных носителей COVID-19». В списке оказались фамилии, адреса, даты рождения и номера телефонов 277 человек, а в качестве основания для контроля приводилась ст.19.5 КоАП (невыполнение в срок законного предписания органа, осуществляющего государственный надзор).

«Сторожевой контроль» — это полицейская база данных, в которую включают сведения о приобретении проездных документов лицами, чьи передвижения подлежат особому контролю. Когда кто-то из них приобретает билет на поезд, самолет или междугородний автобус, ответственному сотруднику полиции направляется уведомление об этом. Созданная в 2005 году секретным приказом МВД система должна была упростить и автоматизировать слежку за экстремистами, однако, как выяснилось впоследствии в ходе рассмотрения Европейским судом дела «Сергей Шимоволос против России», в нее могут включаться сведения о гражданских активистах, правозащитниках и иных лицах. Решение о внесении лица в базу «Сторожевой контроль» принимается на основании «конфиденциальной информации», а процедура его принятия — не известна. Таким образом, созданная для контроля над неблагонадежными гражданами автоматизированная система, вероятно, используется для слежки и за потенциальными распространителями коронавирусной инфекции.

Кроме того, утечки личных данных отмечены в Башкортостане, Дагестане, Якутии, Алтайском крае, Волгоградской, Ростовской, Свердловской, Новосибирской областях и Забайкальском крае.

Во всех случаях разглашалась информация, подлежащая включению в единую базу данных, однако источником утечки (за исключением

ситуации со сведениями о штрафах за нарушение самоизоляции), вероятно, становились люди, имеющие доступ к данным, — сотрудники полиции, Роспотребнадзора, администрации медицинских учреждений и медицинские работники.

Значительное число утечек подтверждает необходимость удаления всех собранных во время режима повышенной готовности сведений о гражданах (за исключением, возможно, обезличенных данных, необходимых для статистического анализа, оценки эффективности предпринимаемых мер и планирования дальнейших действий).

Поскольку полномочия по выявлению контактов пациентов с диагностированной коронавирусной инфекцией и контролю соблюдения карантина переданы региональным властям, Международная Агора и Роскомсвобода обратились к главам субъектов Российской Федерации с предложением гарантировать уничтожение всех собранных персональных данных граждан в установленные законом сроки с определением ответственных должностных лиц. В отношении граждан, помещенных на карантин, — по истечении его срока, а в отношении всех жителей региона — после отмены режима повышенной готовности.

В большинстве регионов посчитали, что специальных гарантий и процедур не требуется, сославшись на положения ст.24 Федерального закона «О персональных данных граждан», согласно которой необходимо прекратить обработку и уничтожить собранные данные в течение 30 дней после достижения целей обработки.

О намерении принять регламент обработки и удаления данных заявили лишь власти Республики Саха (Якутия) и Псковской области. В мае власти Татарстана сообщили об удалении базы данных цифровых пропусков, а вскоре Минкомсвязь России заявила, что все данные, собранные с помощью приложения «Госуслуги СТОП Коронавирус», также удалены.

В любом случае это касается лишь информации, которую собирали для оформления цифровых пропусков в нескольких регионах страны. Медицинские и биометрические данные, а также сведения о контактах собирались и обрабатывались отдельно, процедура их обработки и удаления остается непрозрачной. Таким образом, риск утечек остается значительным.

При этом правительство Москвы уже признало, что собранные для оформления цифровых пропусков данные будут храниться в течение

неопределенного времени — их удаление планируется только «после завершения судебных процедур, касающихся пропускного режима».

Рекомендации

Мы признаем, что беспрецедентный глобальный кризис, с которым столкнулось человечество, требует принятия некоторых чрезвычайных мер, в том числе может оправдывать определенное ограничение прав и свобод человека. Власти всех стран обязаны противостоять пандемии, а общество вправе ожидать, что правительства смогут преодолеть ее экономические последствия и остановить распространение вируса.

В то же время мы убеждены, что любые предпринимаемые меры должны быть законными, эффективными и соразмерными, а ограничение прав и свобод может быть только временным и подлежащим общественному контролю.

Мы призываем российские власти отказаться от чрезмерного расширения вмешательства в право на приватность и уважение частной жизни, а также следовать нормам международного права.

Мы рекомендуем придерживаться следующих принципов:

1) Любая слежка должна быть установлена доступными и понятно сформулированными нормативными актами, принятыми уполномоченными органами в пределах своей компетенции.
2) Использование любых технологий наблюдения должно быть добровольным и не обязательным. Принудительная слежка и сбор информации о частной жизни конкретных лиц должны быть санкционированы мотивированным постановлением суда и быть ограничены по времени, объему и способу осуществления.
3) Массовая неизбирательная слежка в любом случае является незаконной и не должна применяться, поскольку не позволяет провести анализ каждого конкретного случая на предмет необходимости и соразмерности применяемых мер.
4) Любые собранные данные должны быть надежно защищены и использоваться только уполномоченными лицами. Государство должно обеспечить ответственность должностных лиц, виновных в разглашении личных данных, а также справедливую компенсацию пострадавшим.
5) В случае обработки обезличенных данных соответствующий государственный орган или уполномоченное лицо должны иметь

возможность и быть готовы в любой момент подтвердить их обезличенность.

6) Данные должны собираться в минимально возможном объеме только для охраны общественного здоровья и не должны быть предметом продажи (в том числе в обезличенном виде), а также использоваться в иных, в том числе карательных целях.
7) Все собранные данные должны надежно удаляться после достижения целей их обработки в каждом случае. В том числе данные, полученные для контроля соблюдения обязательного карантина конкретными лицами, должны быть уничтожены после прекращения карантина.
8) Слежка не может носить дискриминационный характер и обусловливаться расой, национальностью, гражданством или страной происхождения.
9) На государстве лежит обязанность обеспечить прозрачность всех предпринимаемых мер и действий, создав условия для их независимого общественного аудита с точки зрения влияния на права человека.

Дамир ГАЙНУТДИНОВ
кандидат юридических наук,
правовой аналитик Международной Агоры

AGORA
— Международная правозащитная группа —

Международная правозащитная группа Агора — объединение десятков юристов из нескольких стран, специализирующихся на правовой защите гражданских свобод на постсоветском пространстве.