Covid-1984:
как за нами следили в год пандемии

Pandemic Big Brother

Роскомсвобода

pandemicbigbrother.online

Ключевые тезисы

1 Власти разных стран заключали соглашения с местными операторами связи для передачи данных о геолокации граждан

2 Приложения для отслеживания контактов с зараженными стали одним из самых популярных цифровых решений, запущенных правительствами стран для предотвращения распространения заболеваемости COVID-19

3 Во время пандемии технологии распознавания лиц стали применяться в том числе для выявления нарушителей обязательного карантина

4 В ряде стран, где установка ослеживающих «коронавирусных» приложений являлась обязательной для всех граждан, за отказ установить приложение можно было получить штраф

5 Весной во время всеобщего карантина дроны стали популярным методом наблюдения за соблюдением режима самоизоляции

6 В России с апреля 2020 года власти запустили 4 официальных правительственных приложения для отслеживания контактов с зараженными, выдачи цифровых пропусков и слежкой за гражданами, находящимися на карантине и домашнем лечении

7 За время пандемии в России граждане получили более 1,1 млн штрафов за нарушение ограничений, связанных с коронавирусом

8 В некоторых случаях государственные коронавирусные приложения используются для явной слежки за гражданами и нарушают их право на неприкосновенность частной жизни

9 В России системы автоматических штрафов за нарушение карантинных норм с помощью технологий распознавания лиц и через приложение «Социальный мониторинг» работали с многочисленными ошибками и штрафовали в том числе законопослушных граждан

Авторы

Саркис Дарбинян

Алена Рыжикова

Анна Карнаухова

Роскомсвобода

При поддержке

Содержание

Введение

В части коронавирусных ограничений, связанных с применением цифровых технологий, мы видим некую гонку в 2020 году между правительствами разных стран в том, какие новые технологии могут быть применены для сдерживания распространения пандемии. За 9 месяцев с момента запуска нашей интерактивной карты Pandemic Big Brother мы обнаружили и такие изощренные методы слежки, как дроны, оповещающие о необходимости соблюдать режим самоизоляции, «умные шлемы», способные измерять температуру граждан и даже дирижабли для поиска нарушителей карантина.

Весь мир впервые столкнулся с таким явлением, как общенациональный карантин, а для выхода из дома даже до ближайшего магазина жителям разных стран порой приходилось получать цифровые пропуска и разрешения.

Что касается России, режим самоизоляции впервые был введен в Московской области и Москве в конце марта этого года. Данный режим предполагал запрет покидать дома для всех граждан, за исключением тех, кому необходимо было посещать рабочие места или медицинские учреждения. Также исключением стали походы в магазины, аптеки, а также выгул питомцев. Далее режим самоизоляции также был введен в других регионах России, а за нарушение такого режима, ожидаемо, последовало введение новых штрафов и иных санкций. Пандемия коронавирусной инфекции позволила оправдать расширение инструментов слежки за гражданами и обосновать необходимость сбора огромных массивов данных о жителях больших городов по благородной причине — забота о жизни и здоровье населения.

Начался тотальный контроль и слежка через государственные сервисы, мобильные телефоны и системы видеонаблюдения с функцией распознавания лиц, цифровые пропуска, QR-коды, мобильные приложения, СМС-пропуска, геотаргетинг от мобильных операторов.

Собранный в настоящем докладе перечень мер для сдерживания распространения пандемии коронавируса с использованием цифровых технологий, не является исчерпывающим. Здесь мы говорим о ключевых инструментах, которые кроме заявленных целей использовались также для слежки за гражданами, в том числе незаконно.

Мобильные приложения

Мир

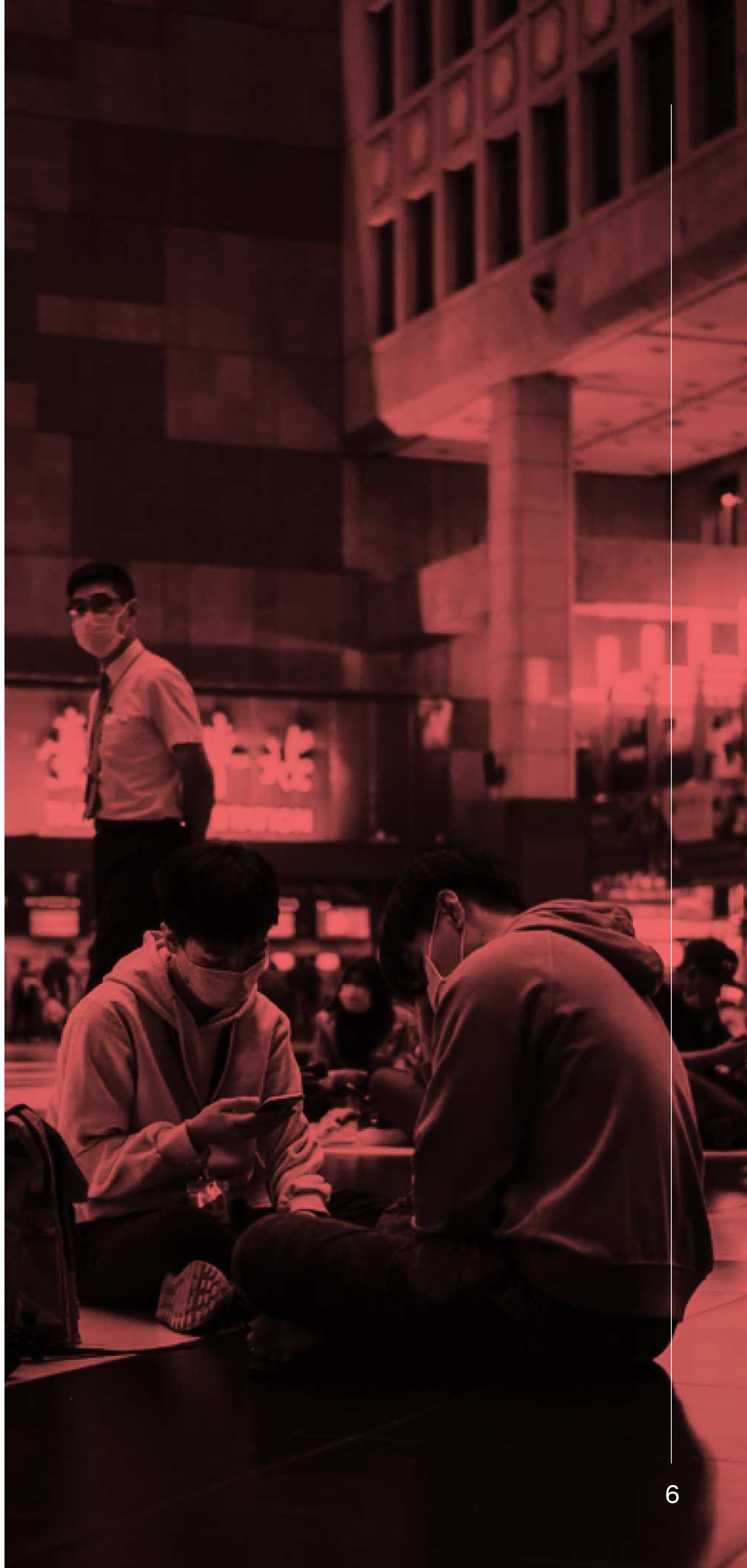
Во всем мире коронавирусные ограничения на передвижения (обязательный карантин, комендантский час) сопровождались и ограничениями цифровыми. Уже с февраля-марта 2020 года власти большинства стран резко активизировали работу своих министерств по цифровизации и цифровому развитию для создания государственных приложений, которые могли бы поспособствовать сокращению новых случаев заболеваемости COVID-19.

С момента запуска и интерактивной карты Pandemic Big Brother во всём мире мы зафиксировали наличие таких приложений в 116 странах мира. В зависимости от преследуемых целей, приложения можно разделить на следующие категории:

Информационные
предоставляют официальную информацию о заболеваемости в регионе, содержат материалы о профилактике заболевания.

Для самодиагностики
позволяют гражданам самостоятельно «продиагностировать» свои симптомы в случаеих наличия и сравнить их с симптомами COVID-19.

Для отслеживания контактов с зараженными
используют технологию Bluetooth или GPS-трекер для фиксации контакта с другими устройствами, находящимися поблизости.



Для отслеживания соблюдения обязательного карантина больными COVID-19
Требуют постоянный доступ к местоположению устройства, могут запрашивать селфи с включенной геолокацией. В некоторых странах помимо обязательной установки приложения пациентов на домашнем лечении обязывают носить специальный GPS-трекер.

Для выдачи цифровых пропусков и QR-кодов, дающих право на выход из дома в период всеобщего карантина.

Используемые правоохранительными органами для отслеживания наличия цифровых пропусков и иных разрешений на время обязательного карантина.

Более 135
государственных приложений запущено для сокращения новых случаев заболеваемости

По состоянию на декабрь 2020 года большинство приложений для отслеживания контактов с зараженными коронавирусом функционируют на основе разработанного совместно Apple и Google API для отслеживания контактов через Bluetooth. Установка приложений, в основе которых лежит эта технология, носит добровольных характер и не является обязательной для всех граждан. В ряде стран зафиксирована широкая заинтересованность в подобных приложениях среди граждан, однако об эффективности такой меры для предотвращения распространения заболеваемости пока мало информации.

Технология, разработанная Apple и Google использует сигнал Bluetooth и оповещает пользователя, если приложением был зафиксирован факт контакта с приложением на другом устройстве, у владельца которого впоследствии подтвердился диагноз COVID-19.

Собираемые данные в этом случае хранятся в большинстве своём децентрализованно на устройствах самих пользователей. Ежедневно каждый телефон генерирует новый закрытый ключ, который впоследствии используется для генерации случайных идентификационных номеров. Если пользователь приложения узнает, что он заражен, он может предоставить органу здравоохранения разрешение публично поделиться своими временными ключами доступа. Сами пользователи при этом остаются анонимными друг для друга.

Не все из зафиксированных нами приложений нарушают право на приватность и другие цифровые права пользователей.

Но большинство из них так или иначе отслеживают местоположение устройства, хранят эту информацию и передают другим устройствам и третьим лицам.

Доступ к технологии будет предоставлен только государственным органам здравоохранения в тех странах, которые решат создать приложение на основе этой технологии. При этом, если они создают приложение, оно должно соответствовать определенным критериям конфиденциальности, безопасности и контроля данных, заданных корпорациями Apple и Google.

Система передаёт собранную о пользователе информацию только в тех случаях, когда он решает сообщить о положительном диагнозе COVID-19 или он получил уведомление о том, что он вступил в контакт с зараженным человеком.

Приложения на основе этого API функционируют в Австралии, Австрии, Бельгии, Бразилии, Германии, Дании, Ирландии, Испании, Италии, Канаде, Латвии, Нидерландах, Польше, России, США (отдельные приложения в каждом штате), Уругвае, Финляндии, Эстонии, Японии и других странах.

Важно отметить, что разработчики европейских приложений, используемых для отслеживания контактов, помимо большого внимания к приватности пользователей и конфиденциальности передаваемых данных, ставят своей целью возможность совместимости приложений друг с другом, в особенности, когда границы между странами вновь будут открыты.

Одной из первых стран, запустивших приложение для отслеживания возможных контактов с зараженными, стал Китай. Приложение Alipay Health Code с момента запуска стало обязательным для всех граждан страны и было интегрировано практически во все сферы взаимодействия людей друг с другом: свой QR-код «здоровья» необходимо предъявлять при посещении публичных мест, поездках в такси, бронировании гостиниц и авиабилетов и т. д. При этом все данные о местоположении автоматически передавали полиции и властям.

Правительство Индии, в которой изначально разрабатывались отдельные приложения в каждом штате, уже к маю сменило тактику и оставило лишь одно приложение — Aarogya Setu — но при этом сделало его обязательным для использования на территории всей страны.

Немецкое приложение Corona Warn ещё в июне стало доступно ещё как минимум в 10 европейских странах:

Люксембурге, Франции, Бельгии, Нидерландах, Австрии, Бельгии, Болгарии, Чехии, Дании, Польше и Румынии.

Отсутствие приложения на смартфоне могло стать основанием для отказа в поездке на поезде или в общественном транспорте, а за отказ от установки приложения граждане могли быть оштрафованы на $13 или привлечены к уголовной ответственности сроком на 6 месяцев. Спустя месяц после запуска приложения 2 апреля количество скачиваний насчитывало уже более 100 млн и приложение вошло в ТОП-10 самых скачиваемых приложений в мире. Позднее после критики со стороны правозащитников о нарушениях права на приватность и сборе конфиденциальных данных, власти заявили, что приложение имеет открытый исходный код.

Также в числе первых разработчиков «коронавирусных» приложений Сингапур с приложением Trace Together. Впоследствии это приложение стало образцом для развертывания подобных систем отслеживания в других странах. Это приложение использует технологию Bluetooth и автоматически удаляет собранные данные через 25 дней. При этом данные из приложения передаются властям только в том случае, если у пользователя по результатам теста подтвердился COVID-19. По состоянию на декабрь приложение загрузили более 50% жителей страны, несмотря на то, что его загрузка носит добровольный характер.

Ряд приложений, запущенных разными странами и преследующих своей целью также отслеживание возможных контактов с зараженными работали по иному принципу и основывались на сканировании QR-кодов (впоследствии такая система была запущена в развлекательных заведениях Москвы).

В начале июня на систему пропусков в общественные места через QR-коды перешла Южная Корея. Одновременно с открытием ресторанов, фитнес-клубов и других общественных пространств владельцев таких заведений обязали установить специальные устройства с QR-кодом, который должны считывать посетители.

Схожая система QR-пропусков также в июне была развёрнута в Тайланде. В местах массового скопления людей и в общественном транспорте появились плакаты с QR-кодами, которые жители страны обязаны сканировать в правительственное приложение, запущенное для отслеживания. За сутки с момента запуска этой системы в ней зарегистрировалось более 44 тыс. бизнес-центров страны.

Шраф $13 или заключение на 6 месяцев могли получить граждане Индии за отказ от установки приложения Aarogya Setu

В конце сентября приложение в том числе с функцией сканирования QR-кодов было запущено в Великобритании. Приложение NHS COVID-19 позволяет отслеживать контакты с зараженным с помощью технологии Bluetooth; оповещает о рисках заболевания, основываясь на почтовых индексах; обеспечивает регистрацию QR-кодов в общественных местах и позволяет проверить свои симптомы на соответствие симптомам COVID-19. Запуск этого приложения изначально был запланирован на июнь, однако несколько раз власти переносили дату из-за нерешённых вопросов с конфиденциальностью собираемых данных. В общественных пространствах страны, как и в Тайланде, были размещены плакаты с QR-кодами, которые посетители должны сканировать в приложение перед посещением.

Помимо Южной Кореи, Таиланда и Великобритании, аналогичная система QR-пропусков также применяется в Гонконге совместно с правительственным приложением «Leave Home Safe».

Отслеживание контактов с зараженными в таких приложениях происходит следующим образом: посетители заведений сканируют QR-код и если у кого-то из посетителей впоследствии обнаруживается коронавирус, остальные получают уведомление о возможном контакте и необходимости соблюдать карантин.

Ещё один тип приложений, на который стоит обратить внимание — приложения для людей, находящихся на домашнем лечении или обязательном карантине.

Власти большинства стран обязывают соблюдать карантин всех жителей, вернувшихся из-за границы. В середине мая приложение для лиц на карантине запустилось в Словакии, нарушителя карантина власти могли оштрафовать на 1650 евро.

Ещё в апреле в Украине было запущено приложение для контроля за соблюдением режима самоизоляции. На протяжении 14 дней пользователям могло приходить до 10 уведомлений в том числе с необходимостью сделать фото.

В Казахстане во время пандемии в мобильное приложение Smart Astana, через которое граждане могут обратиться в столичный Интеллектуальный контакт-центр по коммунально-бытовым вопросам и получить консультацию по государственным услугам, был добавлен ряд новых функций, в том числе для наблюдения за людьми, находящимися на обязательном карантине.

Власти обязали всех, кто находится на карантине установить приложение и включить настройки геолокации, Wi-Fi и Bluetooth, чтобы в режиме реального времени отслеживать их местоположение. При этом сообщается, что в случае отклонения более чем 30 метров от точки, зафиксированной в качестве домашнего адреса, Минздрав получает уведомление об этом и человеку поступает видеозвонок для уточнения местоположения.

> Ряд стран не ограничились лишь внедрением приложений, а запустили ещё более инновационную систему глобальной слежки за гражданами, которая включает в себя браслеты и другие носимые устройства, отслеживающие местоположение.

Таким образом поступило правительство Кувейта, где всех граждан возвращающихся домой из-за границы обязали носить отслеживающие браслеты. Этот браслет также интегрирован с правительственным приложением, регистрация в котором происходит по уникальному государственному идентификатору каждого гражданина. Если браслет фиксирует, что человек вышел за пределы заданной геолокации, службам здравоохранения страны поступает оповещение о нарушении.

Аналогичная система с приложением и браслетами также функционировала в Бахрейне. Однако помимо постоянного отслеживания местоположения, приложение также регулярно запрашивало селфи с подтвержением того, что человек соблюдает обязательный карантин.

В целом тенденция на более жесткие методы отслеживания местоположения граждан с применением браслетов наблюдается в странах Среднего Востока. В соседнем Омане в дополнение к правительственному приложению Tarassud, которое информирует граждан о последних новостях о пандемии COVID-19 в стране, было запущено Tarassud Plus – приложение для людей, находящихся на карантине и обязанных носить специальный браслет. Это приложение автоматически отправляет оповещение властям в случае, если пользователь нарушает карантин или пытается снять или повредить устройство.

Штраф до $55 000 или лишение свободы сроком до 3 лет могут получить жители Катара за отказ от установки правительственного приложения

> Ещё в июне этого года международная неправительственная организация Amnesty International выпустила исследование, в котором сообщалось, что страны Персидского залива под предлогом цифровых коронавирусных ограничений запустили массовую слежку за своими гражданами.

Однако если в арабских странах система контроля за местоположением через браслеты применяется для слежки за гражданами на карантине, то уже упомянутый выше Сингапур распространяет подобную систему на всех жителей страны. По данным очевидцев, власти обязали каждого жителя страны установить приложение для отслеживания или носить с собой специальный брелок, аналогичный по функционалу. Уже с ноября это требуется для входа в кинотеатр, а с начала 2021 года отсутствие приложения или брелка будет являться основанием для отказа в посещении магазинов, метро и других мест скопления людей.

Пожалуй, лидером в слежке за гражданами через правительственные приложения, запущенные в период пандемии коронавируса, стала Сирия. В апреле СМИ сообщали, что под видом коронавирусного приложения правительство распространяет вредоносное ПО. Также были сообщения, что хакеры, связанные с правительством страны, использовали как минимум 71 вредоносное ПО для Android, которое отслеживало местоположение, собирало контакты на устройстве и получало доступ к фото и видео файлам.

Сирия — лидер в слежке за гражданами через правительственные приложения, запущенные в период пандемии коронавируса

Пока правительства одних стран намеренно запускают сомнительные приложения для предотвращения распространения заболеваемости COVID-19, а на самом деле намеренно следят за гражданами, другие приостанавливают работу таких приложений в связи с несоразмерным вмешательством в частную жизнь. Пример такой смены правительственной тактики в борьбе с пандемией – норвежское приложение Smittestopp. Оно было официально запущено в апреле 2020 года, но уже в июне Норвежское управление по защите данных постановило, что постоянное отслеживание геолокации граждан нарушает право на частную жизнь. Работа приложения была приостановлена, а собранные им данные были удалены.

Россия

Российские власти с начала пандемии успели запустить целых четыре приложения, используемых для выдачи цифровых пропусков, слежки за людьми на карантине и отслеживания контактов с зараженными COVID-19.

В апреле Минцифры запустило приложение для выдачи цифровых пропусков регионах «Госуслуги СТОП коронавирус». Авторизация в нём происходила через портал «Госуслуги», а само приложение интересовалось самочувствием пользователя, просило заполнить анкету и указать причину выхода из дома. После указания всех требуемых данных приложение генерировало QR-код и показывало «Таймер пребывания на улице». В ряде регионов были введены собственные пропускные системы, а оформлять разрешения на выход из дома жителей отправили на специальные страницы сайтов местных ведомств.

Москва же, в свою очередь, лидирует по количеству инструментов контроля и слежки: с апреля были введены цифровые пропуска для контроля за перемещением граждан и начала работу система контроля за больными коронавирусной инфекцией «Социальный мониторинг», а в мае сотрудники ГИБДД стали использовать приложение «Карантин» для выявления автомобилей без пропусков.

Пожалуй, самым нашумевшим за время режима самоизоляции в России стало приложение «Социальный мониторинг». Москвичи массово жаловались на ошибки в работе приложения: им приходили автоматические штрафы за нарушение карантина даже в тех случаях, когда они вовсе не покидали свои квартиры или их период карантина уже закончился.

Ранее 4 июня мэр г. Москвы Сергей Собянин заявил, что власти столицы не планируют хранить данные, полученные с помощью системы цифровых пропусков и приложения «Социальный мониторинг», однако продолжают их хранить в течении неопределенного срока. Приложение установили более 400 тыс. москвичей.

Во время роста количества штрафов за нарушение масочного режима и режима самоизоляции юридический сервис Destra Legal запустил приложения для обжалования штрафов за карантинные нарушения. Приложение содержало пошаговое руководство по заполнению жалобы на штраф за нарушение самоизоляции и позволяло в автоматическом режиме направить жалобу в суд.

Далее 11 июня Первый замруководителя аппарата мэра Москвы Алексей Немерюк сообщил о том, что данные граждан из системы цифровых пропусков будут удалены после всех судов, касающихся пропускного режима, что с точки зрения закона представляет из себя достаточно неопределенный срок, учитывая что сроки рассмотрения в судах первой инстанции и в ЕСПЧ сильно отличаются. На данный момент информация по способу и точному сроку удаления данных, о создании спецкомиссии отсутствует, как и любая иная ясная информация о цели сбора данных москвичей.

В конце августа глава российского Минздрава сообщил, что власти начали разработку мобильного приложения, которое будет отслеживать состояние здоровья вакцинированных россиян. Несмотря на то, что по состоянию на декабрь 2020 года, вакцинация от коронавируса в России уже началась, о запуске этого приложения пока нет никакой информации.

> Несмотря на ослабление карантинных мер, в октябре количество инструментов для слежки за жителями Москвы только прибавилось.

Так для развлекательных заведений были установлены специальные требования и с 19 октября гости и работники этих заведений должны были отсканировать QR-код и подтвердить свой номер телефона, либо же отправить СМС-сообщение, так называемая система чекинов.

Руководитель Департамента торговли Алексей Немерюк назвал данную систему «гуманной», так как благодаря идентификации граждане смогут определить угрозу для их жизни и быстрее начать лечение, если вдруг последует заражение.

Далее Мэр Москвы Сергей Собянин в указе обязал работодателей еженедельно передавать данные о работниках, переведенных на удаленный режим работы, а именно: номер мобильного телефона сотрудника; государственный номер автомобиля; номер карты «Тройка» или «Стрелка»; номер социальной карты.

В Департаменте информационных технологий отметили, что власти Москвы не будут контролировать перемещения граждан, данные о которых они получат с помощью вышеуказанных мер. По словам департамента, эта информация нужна только для оперативной оценки эффективности реализации введенных ограничений. Тогда же власти отчитались, что четыре крупных российских компаний (Сбербанк, ВТБ, РЖД и Mail.ru Group) передали мэрии персональные данные более 35 тысяч своих сотрудников, переведённых на удаленный режим работы.

«Роскомсвобода» же в свою очередь подала иск в Мосгорсуд с требованием отменить предусмотренные указом мэра Москвы Сергея Собянина обязательства работодателей передавать данные о работниках, так как это нарушает Закон о персональных данных и Трудовой кодекс. На момент подготовки доклада слушание по делу еще не состоялось.

Четвертым приложением, запущенным российскими властями за время пандемии стало приложение «Госуслуги. COVID трекер» для отслеживания контактов с больными коронавирусом. Несмотря на слово «госуслуги» в его названии с порталом государственных услуг оно никак не связано, а власти уверяют, что собираемая информация носит анонимный характер. Это приложение базируется на технологии Exposure Notification, разработанной Apple и Google, а установка приложения, в отличие от «Социального мониторинга», носит добровольный характер.

Штраф до 300 000 руб. или приостановка деятельности грозили работодателям в Москве

За нарушение требований передавать данные о работниках, переведенных на удаленный режим работы (в соответствии со ст. 20.6.1 КоАП (невыполнение правил поведения при чрезвычайной ситуации или угрозе ее возникновения)

Видеонаблюдение и распознавание лиц

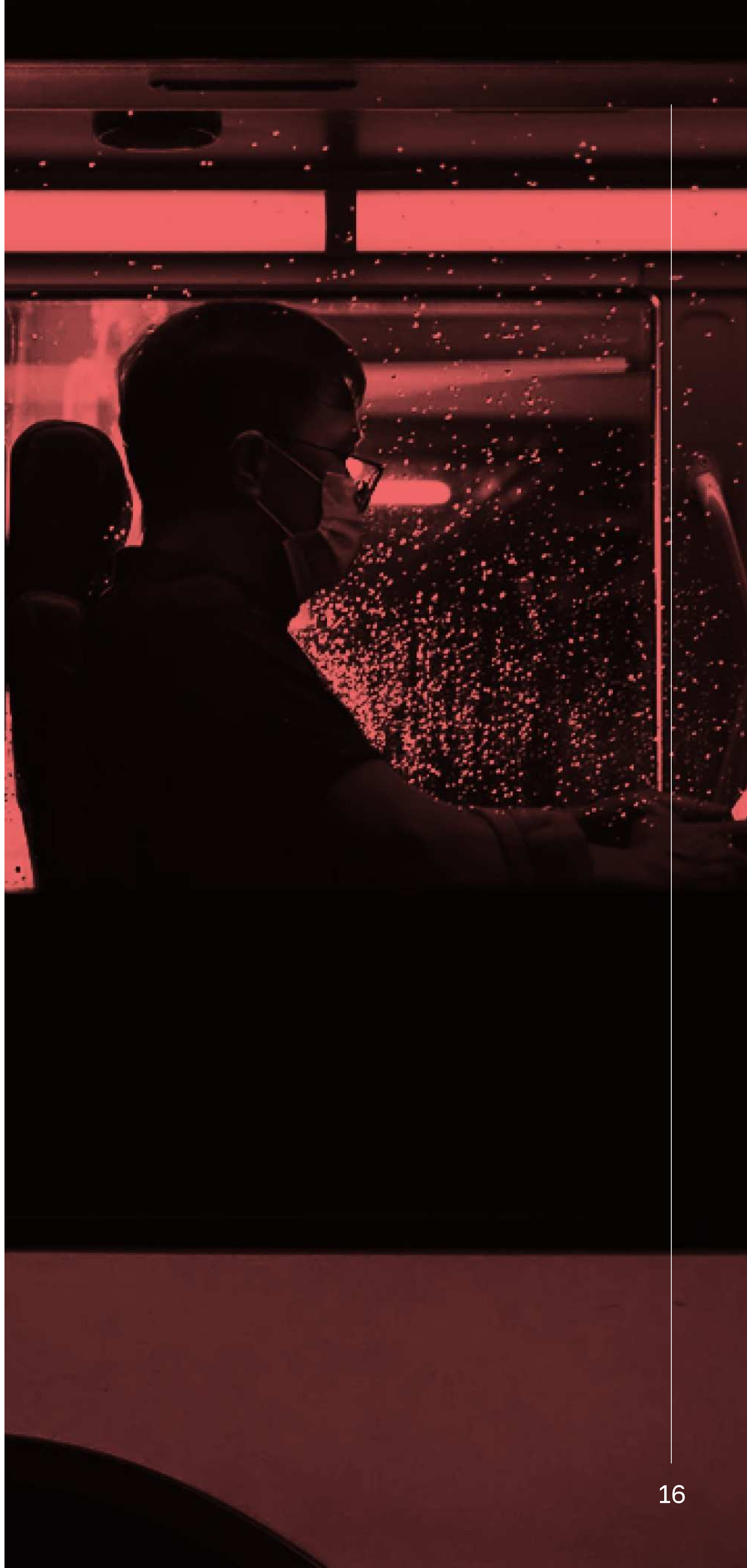
Мир

Практически с самого начала всемирной пандемии коронавируса, мы обнаружили, что правительства разных стран начали использовать системы видеонаблюдения, в том числе с функцией распознавания лиц для наблюдения за соблюдением режима самоизоляции и поимки нарушителей обязательного карантина.

В Китае, где технологии распознавания лиц активно применялись ещё до пандемии коронавируса, камеры отслеживали нарушителей карантина и режима самоизоляции. Используемые в Китае алгоритмы на основе машинного обучения способны распознавать людей в масках и определять наличие температуры.

По внедрению технологий, в частности, технологий для слежки во время пандемии, Китай несомненно вырывается в лидеры. Полицейских в Китае снабдили «умными шлемами», которые автоматически изменяют температуру тела всех вокруг и могут при необходимости сканировать QR-коды граждан. Компания-разработчик сообщила, что уже отправила шлемы в военную полицию Италии и правительство Нидерландов для испытаний. Эти же устройства уже применяются полицией в Дубае.

В сентябре Японская технологическая компания NEC сообщила, что разработала технологию распознавания лиц, которая может с точностью до 99,9% определять лица людей, даже когда они носят маски. Одновременно с этим компания заявила о готовности выпустить эту технологию на рынок, однако первым местом, где эта технология была внедрена, стал главный офис компании в Токио.



В ряде стран для наблюдения за соблюдением ограничений была мобилизирована «армия дронов»

Дроны следили за тем, чтобы люди не собирались большими компаниями и оповещали о необходимости соблюдать самоизоляцию. Впервые дронов для этих целей применил Китай ещё в начале марта. Позднее эту идею переняли и правительства других стран: Австралии, Бельгии, Германии, Греции, Италии, Испании, Казахстана, ОАЭ и США.

В конце апреля власти Индии рассматривали возможность внедрения дронов с функцией распознавания лиц, интегрированных с системой Aadhaar. Это - индийская программа цифровой идентификации, основанная на биометрии, которая насчитывает более 1,25 миллиарда человек, и, возможно, является крупнейшей в мире системой сбора биометрических данных.

В то же время пандемия стала толчком для активного внедрения технологий распознавания лиц в том числе и в демократических странах, а международные правозащитные организации стремятся прийти к диалогу с властями, чтобы доказать, что это излишняя мера, которая нарушает права граждан на частную жизнь.

В ряде стран во время пандемии была протестирована работа систем видеонаблюдения с функцией распознавания лиц. В мае власти Франции в тестовом режиме запустили в работу алгоритмы распознавания лиц в парижском метрополитене. Сообщается, что умные алгоритмы способны распознавать в том числе наличие маски у пассажиров. В Великобритании работа систем распознавания лиц в рамках пилотного проекта была запущена в магазинах.

В настоящее время власти Арабских Эмиратов активно внедряют технологию распознавания лиц в общественном транспорте Дубая. Транспортная полиция города заверяет, что такая мера позволит эффективнее выявлять преступников, однако, как показывает практика других стран, распознавание лиц может использоваться в том числе и для слежки за гражданами.

Бельгия на сегодняшний день является единственной страной, где использование технологий распознавания лиц запрещено на законодательном уровне.

Также стоит отметить случай США, где волна протестов против полицейского насилия Black Lives Matter привела к тому, что крупнейшие технологические компании, разрабатывающие алгоритмы по распознаванию лиц, приостановили продажу этих технологий правительственным органам. На этот шаг пошли, в частности, Microsoft, IBM и Amazon. А в сентябре еще один город в США, Портленд, вслед за Сан-франциско, Оклендом и Сомервиллем, запретил использовать технологию распознавания лиц в общественных местах города. В частности, речь идёт о ресторанах и магазинах. Городской совет Портленда также запретил местным правительственным органам приобретать или применять технологию, которая вызывает в обществе столько споров.

Россия

Россия, и в частности Москва, тем временем стала настоящим полигоном для активного внедрения технологий распознавания лиц в систему городского видеонаблюдения. За последние полгода власти Москвы потратили почти 1,5 млрд рублей на оснащение общественного транспорта камерами с функцией распознавания лиц. Позднее в столичном МВД заявили, что защитные маски не мешают камерам распознавать лица.

При этом с введением пропускного режима в столице более тысячи камер видеонаблюдения были подключены к системе для контроля режима самоизоляции. Оператором системы видеонаблюдения стала квази-государственная организация ОАТИ, которая осуществляет функции по контролю перемещения граждан, находящихся на обязательном карантине с выставлением автоматизированных штрафов, принятых на основании алгоритмов, связанных с работой модуля по идентификации лица гражданина. Изображения гражданина с видеопотока сравнивается с фотографией, которая производится во время первого визита врача. Впрочем, наличие вероятности в 74% совпадения лица не мешало судам оставлять в силе решения ОАТИ по назначению гражданам административных штрафов.

С начала пандемии коронавирусной инфекции в России были привлечены к административной ответственности более 1,1 млн граждан за нарушения ограничений, введенных с целью борьбы с распространения коронавируса COVID-19.

С 1 апреля в КоАП Москвы введена ответственность за нарушение режима самоизоляции (ст. 3.18.1 КоАП Москвы). Наказание по данной статье предусматривает штраф для граждан в размере 4 тыс. руб.

Более 109,2 тыс. протоколов было выписано по ст. 3.18.1 КоАП Москвы. Многие из граждан были признаны виновными только на основании данных, полученных с помощью городских камер видеонаблюдения. Дела о таких нарушениях рассматриваются без составления протокола об административном правонарушении. Для идентификации нарушений на дорогах города используется номер автомобиля, а вот личность пешехода подтверждают по фотографии. Ожидаемо, что использование таких технологий привело к массе ошибок и, в итоге, несправедливым и незаконным штрафам, которые до настоящего времени обжалуются в судах.

По данным картотеки Мосгорсуда были обжалованы более 64 тыс.штрафов по ст. 3.18.1 КоАП Москвы, из них:

- отменены более 73 решения;
- завершено 1 250 дел;
- обжаловано 123 штрафа;
- возвращено 13 564 жалоб;
- вступили в силу 2 213 решений;
- прекращены дела по 10 125 штрафам;
- назначено судебное заседание 1 673 жалоб.

В Подмосковье в период майских праздников Росгвардия применяла дроны для отслеживания соблюдения режима самоизоляции, а позднее для этих целей и вовсе запустила аэростат.

Жители российских регионов также успели ощутить на себе все «прелести» государственной слежки в период обязательной самоизоляции.

Дочерняя компания «Ростеха» разработала систему видеоаналитики, способную отслеживать соблюдение масочного режима, и она была внедрена как минимум в нескольких регионах: в Нижегородской и Сахалинской областях, в Санкт-Петербурге и в Республике Татарстан.

Как и москвичи, жители Южно-Сахалинска столкнулись с автоматическими штрафами за нарушение карантина, которые были выписаны на основе данных с камер видеонаблюдения. И здесь также не обошлось без ошибок в работе алгоритмов.

Геотаргетинг

Мир

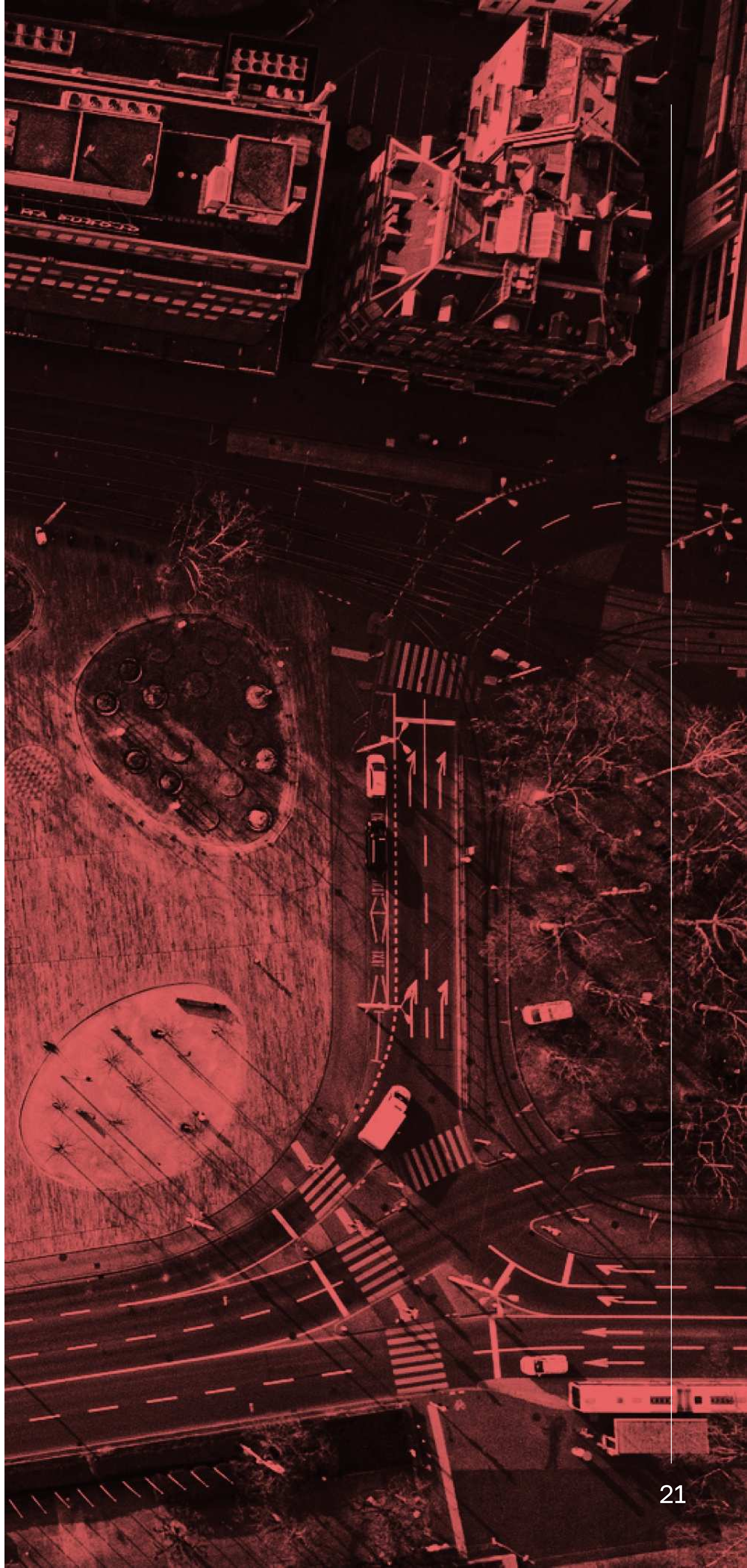
Правительства разных стран используют данные о местоположении пользователей интернета и абонентов сотовой связи для того, чтобы отследить как распространяется вирус и работают ли принятые меры о необходимости соблюдения социальной дистанции.

Данные о местоположении пользователей могут быть собраны различными способами, в том числе через операторов сотовой связи. Если отслеживание через технологии Bluetooth и GPS-трекеры осуществляется через сторонние приложения, то данные о местоположении по базовым станциям собирают и хранят операторы сотовых данных.

Ещё до появления приложений для отслеживания контактов с зараженными COVID-19, правительства ряда стран признались, что сотрудничают с местным операторами связи для отслеживания перемещений граждан.

В марте один из крупнейших европейских операторов Vodafone подтвердил, что передавал правительству данные о геолокации своих абонентов для составления агрегированной анонимной тепловой карты перемещений в регионе Ломбардия (Италии), чтобы помочь властям лучше понять движения населения и предотвратить распространение COVID-19.

Позднее уже 8 европейский операторов сотовой связи согласились предоставлять Еврокомиссии данные о передвижениях для прогнозирования распространения заболеваемости COVID-19. Еврокомиссия в свою очередь заявила, что данные будут использоваться в обезличенном виде и будут удалены по окончанию пандемии.



Ещё в середине марта правительство Израиля предоставило полномочия службе контрразведки и внутренней безопасности на запрос у операторов сотовой связи данных об абонентах, в том числе их местоположение, а также право на обработку этих данных для выявления возможных контактов с носителями вируса. В случае выявления возможных контактов власти рассылали на указанные номера телефонов сообщения о необходимости соблюдать карантин. Впоследствии верховный суд постановил, что для использования этой меры предупреждений в рамках закона правительству необходимо выпустить специальный закон «о приватности», который бы позволял властям такое вмешательство в частную жизнь граждан. Несмотря на то, что уже в апреле в стране было запущено приложение, которое фактически преследовало те же цели, программа по отслеживанию местоположения граждан на основе данных сотовых операторов была свёрнута лишь в июне.

В начале апреля правительство ЮАР сообщило, что будет использовать данные сотовых операторов для отслеживания возможных контактов с зараженными Covid-19. При этом врачей обязали предоставлять властям всю информацию о больных пациентах, в том числе их имена, телефоны и домашние адреса.

Ещё в марте президент Сербии, объявив чрезвычайное положение в стране позволил властям получать доступ местоположению всех граждан на основе данных мобильных операторов.

Парламент Армении также обязал операторов сотовой связи предоставлять данные о всех абонентах, в том числе номера телефонов и точное местоположение, а также детализацию звонков и смс-сообщений. Эта информация впоследствии использовалась для наблюдения и выявления контактов с больными COVID-19.

В Азербайджане не без помощи сотовых операторов была запущена система смс-пропусков. Всякий раз перед выходом из дома жителям страны необходимо было звонить или отправлять смс на специальный номер с указанием цели выхода. Собранные данные передавались сотрудникам полиции, а те в свою очередь могли останавливать на улицах для проверки наличия разрешений. В декабре с ростом числа заболевших система смс-пропусков была вновь восстановлена.

В Латвии полицейским и Центру по профилактике и контролю заболеваний предоставили возможность запрашивать данные о местоположении граждан у сотовых операторов

В случаях, когда им необходимо убедиться в достоверности данных, указанных пациентами.

В апреле в Казахстане крупнейшая в стране телекоммуникационная компания предложила создать систему отслеживания передвижений граждан за пределами мест их проживания на основе данных мобильных операторов. Управление цифровизации Акимата г. Алматы и местные сотовые операторы заключили соглашение о сотрудничестве в рамках мер по противодействию распространения коронавируса. В результате чего был составлен геолокационный анализ, который отображает активность абонентов мобильных операторов и выявляет места скопления абонентов на ежечасной основе. Среди данных, передаваемых сотовыми операторами властям была в том числе и звонковая активность абонентов, что указывает на нарушение конституционного права на неприкосновенность частной жизни.

> Южная Корея ещё на раннем этапе распространения коронавируса создала в стране общедоступную базу данных о выявленных случаях коронавируса, которая предоставляет подробную информацию о каждом инфицированном человеке, включая точные передвижения по стране на основе данных от сотовых операторов.

Эта база данных постоянно обновляется в том числе с использованием информации о местоположении из транзакций по платежными картами, данных сигналов мобильных телефонов и видеозаписей с камер видеонаблюдения.

Власти Тайваня взяли под контроль местоположение людей, находящихся на обязательном карантине. Департамент кибербезопасности страны отслеживает телефонные сигналы граждан и оповещает полицию и местных властей, если люди, находящиеся на домашнем карантине, удаляются со своего адреса или выключают свои телефоны. Сообщается, что полиция связывается или наведывается к тем, кто нарушает карантин, в течение 15 минут.

В США компании, предоставляющие услуги мобильной рекламы, сотрудничали с Центрами по контролю и профилактике заболеваний, а также с правительствами разных штатов и местными властями, чтобы проанализировать, как изменились передвижения людей на основе данных о местоположении мобильного телефона. Корпорация Google выпустила отчеты о передвижениях людей во всем мире, которые были основаны на данных о местоположении, собранных Google Maps. Эти данные передавались в том числе и контролирующим органам для составления прогнозов распространения заболевания и анализа соблюдения мер социальной дистанции.

Сбор данных о местоположении пользователей также был замечен нами в Австралии, Испании, Чехии, Великобритании, Бразилии, Эквадоре, Словакии, Швейцарии, Китае, Иране, где правительство объяснило это защитой населения и предотвращением риска развития и распространения COVID-19.

Россия

В России 20 марта премьер-министр поручил Минкомсвязи разработать общенациональную систему для отслеживания граждан, контактировавших с больными коронавирусом, на основе данных операторов сотовой связи.

30 марта Минкомсвязь потребовала от региональных властей предоставить обезличенные списки номеров мобильных телефонов людей, инфицированных коронавирусом. Помимо больных с подтвержденным диагнозом, ведомство также интересовали номера телефонов лиц, находящихся на обязательном карантине по возвращению из-за границы. В последнем случае по каждому номеру телефона операторы связи предоставили ведомству информацию о странах и местах, которые посещал абонент, а также дату возвращения в Россию.

1 апреля министерство отчиталось о выполнении. Оно запросило у региональных властей обезличенные списки мобильных номеров носителей коронавируса и людей, находящихся на самоизоляции после возвращения из-за рубежа или контактов с подтвержденными носителями.

Специальный алгоритм составляет список тех, кто находился рядом с больным, а также тех, кто общался с ним по мобильной связи в течение двух недель. Если система распознает, что какой-то абонент находился вместе с зараженным в течение минимум пяти минут, то его номер попадает в базу. Если абонент контактировал с больным коронавирусом, то система направит ему об этом СМС-сообщение. В нем будет также указано, что человеку нужно самоизолироваться. Данные абонента отправят в региональный оперштаб и будут отслеживать его местоположение.

> Основным источником сбора данных о гражданах для государства остаются операторы мобильной связи

Десятки миллионов абонентов примерно каждые 5 минут отправляют сигнал на базовые станции. При наложении данных о геолокации на карту города можно получить маршруты перемещения пользователей. Погрешность при этом составляет 50–100 метров, которые добавляют сами системы.

Министр цифрового развития, связи и массовых коммуникаций Максут Шадаев рассказал, как осуществлялся контроль за гражданами, прибывшими из-за рубежа в начале эпидемии коронавируса. По его словам, по соглашению с операторами мобильной связи власти брали под контроль сим-карты вернувшихся в страну. Далее при помощи мобильного оператора власти определяли место пребывания человека и направляли сообщения о необходимости соблюдать самоизоляцию.

Заключение

Принимаемые разными странами инструменты для предотвращения распространения COVID-19 не всегда были соразмерны целям, которые эти меры должны были достигнуть. Ускоренный запуск приложений для отслеживания контактов и контроля за гражданами на карантине приводил к тому, что эти приложения работали с ошибками и далеко не во всех случаях оповещали людей о необходимости соблюдать карантин или штрафовали за нарушение карантина в тех случаях, когда в действительности нарушений не было.

2020 год показал возможности совершенно новых технологичных способов слежки за населением с комбинированием сразу многих методов сбора и аналитики данных. Возможности ИИ и машинного обучения использовались государствами для контроля и административного преследования за нарушения ограничений по передвижению. При этом, персональные данные, которые собирались многими государствами Ближнего Востока и Азии, далеко не всегда соответствовали принципу пропорциональности и необходимости. Анализ эффективности принятых мер по сбору больших массивов данных о граждан с изучением корреляции по количеству зараженных/умерших является предметом самостоятельного исследования, однако до настоящего момента таких данных не имеется. Среди стран региона Россия и Казахстан, пожалуй, остаются лидерами по количеству применяемых цифровых технологий контроля за перемещением граждан.

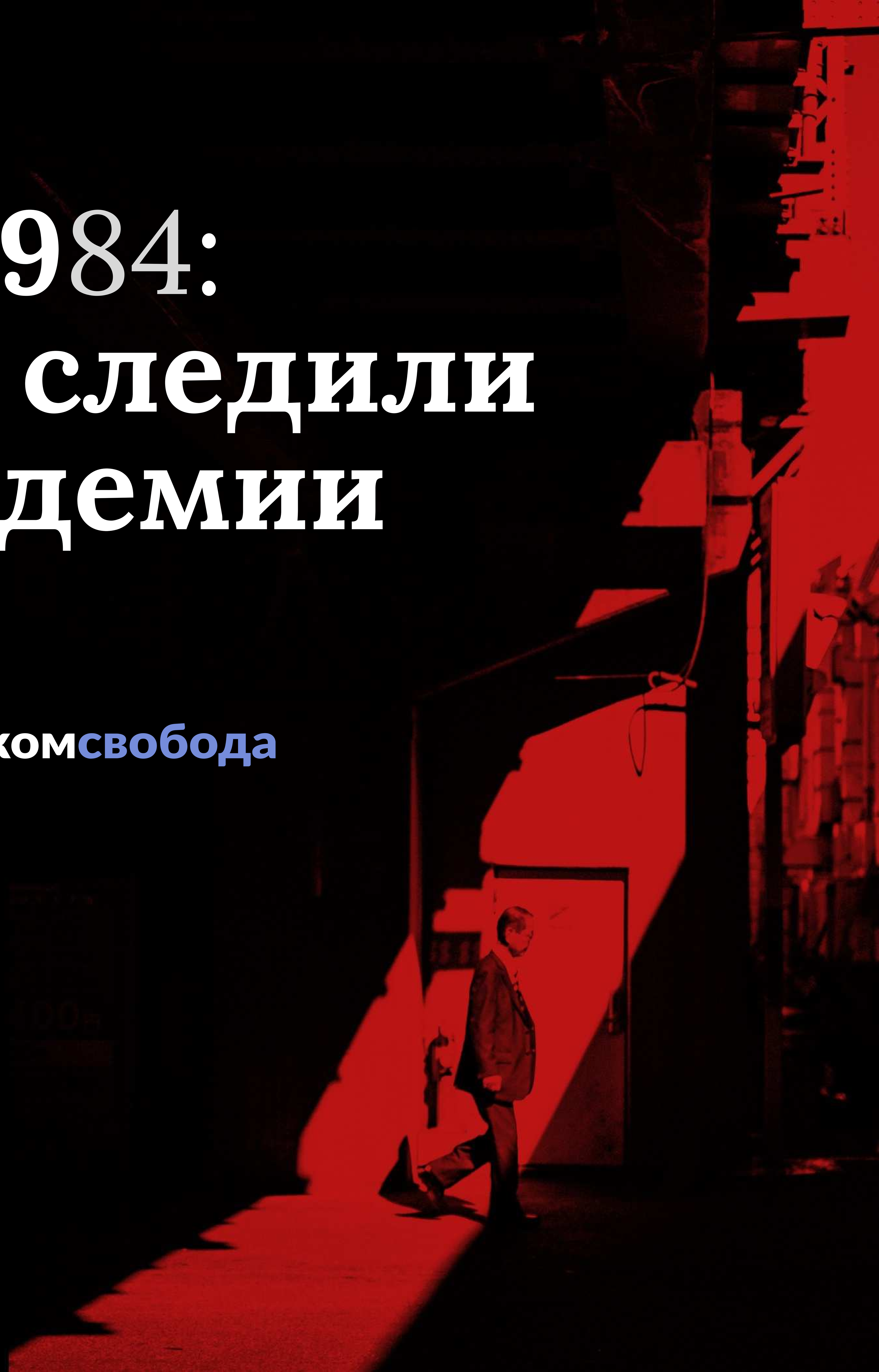
Серьезные риски утраты тайны частной жизни и примеры принимаемых ограничений в других странах привели европейское сообщество к пониманию необходимости укрепления правовой позиции в Европе в части массового сбора данных. В октябре 2020 Европейский суд справедливости вынес знаковое решение, по которому серьезно ограничил правительства стран ЕС, в том числе правоохранительные органы и спецслужбы в массовом постоянном сборе пользовательских данных через мобильных и интернет-провайдеров, а также хранении этих данных. Исключение допускается лишь при наличии угрозы национальной безопасности. При этом, суд подчеркнул, что сбор данных для противодействия такой угрозе должен быть ограничен во времени и сопровождаться эффективными гарантиями осуществления надзора со стороны судов или независимых административных органов.

14 декабря 2020 глава Минздрава Великобритании Мэтт Хэнкок сообщил, что британские ученые выявили новый, мутировавший, тип коронавируса, который распространяется быстрее известных штаммов и который на 70% заразнее, чем другие виды вируса. С 20 декабря в Лондоне и некоторых частях Великобритании начал действовать 4-ый максимальный уровень ограничений, предусматривающий закрытие всех заведений (кроме продающих товары 1-ой необходимости). Транспортное сообщение многих стран уже ограничено. И их список постоянно растет.

В то же время, Главный санитарный врач России Анна Попова продлила период действия санитарно-эпидемиологических правил по профилактике коронавирусной инфекции до 2022 года постановлением от 13.11.2020 № 35. В зависимости от эпидемиологической ситуации каждый субъект федерации может устанавливать свои ограничения.

Исходя из тенденций на момент публикации отчета инструменты слежки в 2021 году будут только увеличиваться. Ограничения прав и свобод граждан с применением цифровых технологий и возможностей операторов связи вряд ли будут сняты в ближайшее время. Будучи апробированным в 2020 году, многие из инструментов, описанных в этом докладе, будут далее совершенствоваться органами государственной власти и могут быть поставлены в арсенал инструментов слежки на постоянной основе.

Covid-1984:
как за нами следили в год пандемии



Pandemic Big Brother

pandemicbigbrother.online

Роскомсвобода

2020