МОСКОВСКИЙ ЦЕНТР КАРНЕГИ

МАРТ 2021

Технологии слежения в России и Евразии. Ожидает ли нас общество тотального контроля?

НИКОЛАЙ МАРКОТКИН

ВВЕДЕНИЕ

Пандемия коронавируса и связанные с ней карантинные меры спровоцировали значительное усиление цифрового контроля, который испытали на себе граждане во многих странах. Среди его инструментов — отслеживание передвижения и контактов людей с помощью данных мобильных операторов; сбор персональных данных; использование камер, подключенных к системе распознавания лиц, и целый ряд других технологий. Активное внедрение государства на территорию, которая еще вчера была личным пространством, вызывает у людей закономерное беспокойство. При этом пандемия стала лишь толчком для наглядной демонстрации технологий, уже несколько лет активно применяемых в крупных мировых мегаполисах.

В Москве технологии, позволяющие эффективно следить за гражданами, были внедрены еще в 2015–2020 годах. В Китае и ряде стран Евразии, таких как Республика Корея, Тайвань и Сингапур, цифровой контроль уже давно стал для жителей привычной реальностью. Борьба с пандемией во многом легитимировала использование технологий слежения, которые теперь воспринимаются как средство обеспечения общественной безопасности, будь то борьба с преступностью или противодействие распространению вируса. И есть основания ожидать, что Россия — в числе многих

других стран — сохранит усиленный цифровой контроль и после эпидемии.

МОСКОВСКОЕ ПОЛЕ ИИ-ЭКСПЕРИМЕНТОВ

Для испытания технологий цифрового управления городом российское руководство выбрало Москву — наиболее крупный и современный российский мегаполис. В 2003–2017 годах в столице была реализована городская целевая программа «Электронная Москва», в 2011–2017-м — государственная программа «Информационный город». Целью первой стало обновление цифровой техники у госслужащих и модернизация инфраструктуры связи. Вторая была направлена на автоматизацию городских процессов и цифровизацию услуг, в том числе медицинских и образовательных.

Реализация этих программ позволила правительству Москвы создать систему сбора и анализа данных о перемещениях горожан, их здоровье, обучении, использовании различных госуслуг. Сегодня в распоряжении московской мэрии около 170 информационных систем. Интересно, что Сергей Собянин еще до назначения мэром Москвы в 2010 году курировал программу «Информационное общество» на должности Руководителя Аппарата Правительства Российской Федерации.

В 2018 году Департамент информационных технологий (ДИТ) представил после обсуждения с бизнесом и населением цифровую стратегию Москвы «Умный город — 2030». В центре стратегии — искусственный интеллект, который анализирует данные из различных источников и предоставляет готовые решения правительству и бизнесу. При этом ключевым поставщиком информации о перемещениях москвичей служат операторы сотовой связи. В частности, их данные позволяют выявлять реальное место жительства горожан, которое зачастую не совпадает с местом регистрации.

Департамент информационных технологий Москвы при посредничестве Аналитического центра при Правительстве РФ с 2015 года закупает геоаналитику у сотовых операторов. К ней относятся данные о перемещении горожан по движению их SIM-карт. По словам заместителя мэра Москвы Максима Ликсутова, город собирает эту информацию, чтобы отслеживать пассажирские потоки и оптимизировать работу общественного транспорта. Мэрия также использует информацию о перемещениях такси, записи камер фото- и видеофиксации, а также дорожных камер, сведения о поездках владельцев карт «Тройка», данные из публичных сетей Wi-Fi.

В 2015–2018 годах ДИТ потратил на покупку геоаналитики 516 млн рублей. Всего же на программу «Информационный (с 2019 г. — Умный) город» в 2012–2020 годах из бюджета Москвы было выделено 500 млрд рублей. При этом Максим Ликсутов утверждал, что столичные власти получают «обезличенные» данные, не привязанные к конкретному гражданину. «У нас нет никаких персональных данных. Эти данные выглядят как точки, которые каким-то образом перемещаются, мы даже близко не знаем, кто это», — подчеркивал московский вице-премьер в комментариях СМИ.

Сбор данных о перемещениях горожан — довольно распространенная практика в современных мегаполисах. В то же время исследование американских и бельгийских ученых еще в 2013 году

показало, что для идентификации человека с точностью 95% достаточно всего четырех точек его местонахождения. Таким образом, можно говорить о том, что подобные данные не являются абсолютно обезличенными и при желании могут быть использованы для сбора информации о передвижениях конкретных людей. При этом мэрия вплоть до весны 2020 года не запрашивала у москвичей разрешение на использование данных об их перемещениях, что делало ее действия сомнительными с легальной точки зрения.

Внедрение технологий слежения, в том числе основанных на использовании искусственного интеллекта, значительно ускорилось в 2020 году на фоне пандемии коронавирусной инфекции. В конце апреля, в разгар первой волны эпидемии, в крайне сжатые сроки был принят Федеральный закон «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве». Тогда же изменения, уточняющие порядок и правовой режим использования обезличенной информации, были внесены в Федеральный закон «О персональных данных». Согласно новому закону, с 1 июля 2020 года в российской столице на 5 лет устанавливалось специальное регулирование, цель которого — создать условия для разработки и внедрения технологий ИИ и последующего использования результатов их применения.

Заявленные в законе цели эксперимента в целом соответствуют проводимой правительством политике последовательной цифровизации госуправления и услуг для населения. Первые три цели:

- обеспечение повышения качества жизни населения;
- повышение эффективности государственного или муниципального управления;
- повышение эффективности деятельности хозяйствующих субъектов в ходе внедрения технологий искусственного интеллекта.

На их фоне выделяется четвертая цель, сформулированная как «формирование комплексной системы регулирования общественных отношений, возникающих в связи с развитием и использованием технологий искусственного интеллекта, по результатам установления экспериментального правового режима». При этом экспериментальный правовой режим предполагает создание «цифровых песочниц», в которых можно отрабатывать технологии, пока еще не регулируемые действующим законодательством.

Законом предусмотрена «защита прав и свобод человека и гражданина, обеспечение безопасности личности, общества и государства». В то же время нельзя не отметить, что расплывчивость формулировок вызывает опасения относительно использования мэрией персонифицированных данных горожан. В частности, в период первой волны пандемии весной — летом 2020 года правительство Москвы следило за перемещением больных коронавирусом и находящихся на карантине граждан с помощью геолокации. Для этого Департамент информационных технологий города еще до принятия закона об эксперименте с использованием ИИ внедрил специальное приложение «Социальный мониторинг».

БЕЗОПАСНОСТЬ ПОД ВИДЕОНАБЛЮДЕНИЕМ

Одновременно с закупкой данных о перемещениях граждан в Москве в 2010-е годы происходило масштабное внедрение городской системы видеонаблюдения (примечательно, что она не была прописана в стратегии «Умный город — 2030»). Уже к 2012 году было сформировано ядро централизованной системы, после чего власти стали активно наращивать количество городских камер. Только за 2018 год к столичной системе было подключено свыше 7 тысяч камер. Всего же в Москве к началу 2019 года насчитывалось чуть менее 170 тысяч камер, установленных во дворах, в подъездах, парках, школах, поликлиниках, магазинах, рынках, на стройках, в офисах органов исполнительной власти и других общественных местах. За следующий год количество камер возросло до 178 тысяч, еще 9 тысяч предполагалось установить в течение 2020 года. Итоговую численность камер еще до пандемии планировали довести до более чем 200 тысяч. Кроме того, они были установлены в общественном транспорте.

Впрочем, необходимо заметить, что даже такое впечатляющее количество камер является относительно скромным по мировым масштабам. Многие мегаполисы мира, особенно расположенные в азиатских странах, обладают значительно более разветвленной сетью видеонаблюдения. Согласно результатам исследования компании Surfshark, по численности камер на 1 квадратный километр Москва сегодня находится лишь на 30-м месте в мире, уступая даже мексиканской Гвадалахаре и аргентинскому Буэнос-Айресу. В топ-10 городов с наибольшей плотностью камер вошли 6 китайских и 3 индийских мегаполиса. Среди западных городов лидируют Лондон и Париж — 4-е и 12-е места соответственно. По общей численности камер российская столица занимает 23-е место в мире. Для сравнения: в Пекине и Шанхае более 1 млн, а в Лондоне — свыше 627 тысяч камер.

Московская мэрия обосновывает создание системы видеонаблюдения преимущественно соображениями безопасности. В частности, в январе 2019 года Сергей Собянин писал в своих соцсетях, что «записи с камер используются в расследовании порядка 70% правонарушений». В качестве меры повышения общественной безопасности московские власти планируют также внедрить одну из «крупнейших в мире» систем распознавания лиц. Столичная система использует программу FindFace, разработанную компанией NtechLab (12,5% принадлежит госкорпорации «Ростех», 25% — фонду Рубена Варданяна, оставшаяся доля — шести акционерам). Ранее также сообщалось о планах московских властей использовать программу FaceControl, созданную российской компанией Vocord, базирующейся в технопарке «Сколково». Однако в июне 2019 года патенты, оборудование и команда разработчиков Vocord были приобретены китайской корпорацией Huawei.

Впервые чуть более тысячи московских камер было подключено к системе распознавания лиц еще в 2017 году, однако настоящей проверкой для системы стал чемпионат мира по футболу 2018 года. В преддверии мундиаля она была в тестовом режиме запущена в столичном метро и тестировалась также в нескольких других городах. Согласно данным госкорпорации «Ростех», за время проведения чемпионата было задержано 180 правонарушителей из федеральных баз данных. Результат экс-

перимента был признан успешным, что открыло дорогу для дальнейшего внедрения системы.

Уже в 2019 году было анонсировано подключение к ней уличных камер наблюдения. Полноценный запуск системы распознавания лиц состоялся в январе 2020 года. К этому моменту к ней были подключены 105 тысяч умных городских камер. Технология FindFace позволяет опознать личность человека, даже если его лицо частично скрыто (например, маской), а также определить такие биологические параметры, как возраст. Таким образом, к началу пандемии московские власти подошли во всеоружии и имели целый ряд отработанных инструментов слежки за перемещениями и иными действиями горожан.

Система продолжает постоянно дорабатываться и совершенствоваться. В частности, в январе 2021 года было объявлено о внедрении в московском метро системы оплаты проезда по лицу пассажира (то есть с помощью системы распознавания). В то же время от создания системы, отслеживающей передвижения пешеходов с помощью аппаратно-программных комплексов на остановках общественного транспорта и информационных стелах, по-видимому, решено отказаться. Последние обновления операционных систем Android и iOS делают сбор необходимой информации (MAC-адресов смартфонов) практически невозможным.

При этом необходимо отметить, что городской контроль наиболее эффективен в формате двухфакторной модели наблюдения, в которой распознавание лиц сочетается с геолокационными данными сотовых операторов. Такая модель позволяет более точно определить местоположение человека, которого необходимо распознать на улице, и значительно облегчает работу правоохранительных органов. В феврале 2021 года Министерство цифрового развития, связи и массовых коммуникаций РФ предложило внести поправки в Федеральный закон «О связи», которые выводят информацию о местоположении мобильного устройства из-под действия тайны связи. Предполагается, что данная инициатива облегчит поиск пропавших людей. Тем не менее в случае принятия законопроекта полиция получит, по сути, неограниченный доступ к геоданным граждан по всей России.

ПАНДЕМИЯ КАК АПОФЕОЗ СИСТЕМЫ СЛЕЖЕНИЯ

Пришедшая в Россию в первой половине 2020 года пандемия коронавирусной инфекции открыла правительству беспрецедентно широкие возможности контролировать население. Одновременно эпидемия стала стресс-тестом для системы слежения, созданной в Москве. Запуск этой системы состоялся в январе, до введения карантинных мер, и изначально она не была рассчитана на обработку такого большого объема данных.

Первоначально на самоизоляцию попадали люди, вернувшиеся из-за рубежа. ДИТ и Департамент здравоохранения Москвы с середины марта начали отправлять им адресные сообщения и электронные письма с требованием оставаться дома. По соглашению с операторами сотовой связи на контроль стали брать SIM-карты всех, кто в этот период возвращался в Россию. 26 марта обязательный режим самоизоляции был введен для пожилых людей старше 65 лет и лиц, страдающих хроническими заболеваниями. 29 марта он был расширен на

всех жителей столицы. С этого момента они могли покинуть дом только для того, чтобы обратиться за экстренной медицинской помощью, поехать на работу, сходить в аптеку или магазин, выгулять собаку или вынести мусор. 2 апреля за нарушение режима самоизоляции были установлены штрафы, 15 апреля введена система цифровых пропусков для перемещения на личном и общественном транспорте. 23 апреля было запущено приложение ДИТ Москвы «Социальный мониторинг» для контроля заболевших людей, лечившихся дома (в ограниченном режиме оно внедрялось уже с начала апреля). Окончательно пропускной режим в Москве был отменен 9 июня.

Несмотря на некоторые сбои, такие как лишние штрафы или очереди в метро, возникшие в день введения электронных пропусков, столичные власти в целом успешно справились с локдауном. Система цифрового контроля тестировалась и совершенствовалась буквально в боевом режиме и к концу режима строгих ограничений функционировала уже без существенных накладок.

В регионах к отслеживанию активности граждан отнеслись «творчески». Многие, правда, как Московская область, копировали меры, принятые Москвой. Другие шли в авангарде применения цифровых инструментов: например, Татарстан первым в России установил систему цифровых пропусков для всех жителей. В целом электронные пропуска были введены с разной степенью эффективности в нескольких регионах. На Сахалине штрафы за нарушение самоизоляции выписывали в полуавтоматическом режиме на основе данных с камер наблюдения. В Красноярском крае МЧС рассылало жителям СМС-сообщения с призывом вернуться домой и не подвергать опасности окружающих.

В некоторых регионах к контролю подошли еще более решительно: к примеру, в Мурманской области на тех, кто проходил лечение на дому, надевали электронные браслеты.

В основном руководство России высоко оценило работу регионов, и в особенности правительства Москвы, по борьбе с пандемией. По всей видимости, эффективными также были признаны методы цифрового контроля за гражданами. Его ключевые инструменты, такие как система распознавания лиц, отслеживание перемещений граждан с помощью геолокации, ограничение свободы слова с помощью статьи Уголовного кодекса РФ о фейковых новостях[1], остались в распоряжении правительства и после снятия основных карантинных ограничений.

ПОЛИТИКА И ЦИФРОВОЙ КОНТРОЛЬ

Серия протестов и революций на Ближнем Востоке в начале 2010-х годов, получившая в СМИ наименование «арабская весна», ярко продемонстрировала мобилизационный потенциал интернет-площадок, в особенности соцсетей. Хотя Twitter и разнообразные мессенджеры не были первопричиной беспорядков, они во многом сыграли роль их детонатора и послужили ключевым инструментом координации протестных действий. Руководство России оценило события «арабской весны» негативно, традиционно увидев в них следы западного вмешательства и манипуляций. Владимир Путин, занимавший тогда должность председателя правительства, в своей статье «Россия и меняющийся мир» (2012) охарактеризовал Интернет и соцсети как действенный политический инструмент:

«„Арабская весна“ также ярко продемонстрировала, что мировое общественное мнение в нынешнее время формируется путем самого активного задействования продвинутых информационных и коммуникационных технологий. Можно сказать, что интернет, социальные сети, мобильные телефоны и т. п. превратились — наряду с телевидением — в эффективный инструмент как внутренней, так и международной политики. Это новый фактор, требующий осмысления, в частности для того, чтобы, продвигая и дальше уникальную свободу общения в интернете, уменьшить риск его использования террористами и преступниками».

Политические протесты в России в 2011–2012 годах выявили неготовность правоохранительных органов к превентивному предотвращению протестных акций и эффективному поиску их участников. 6 мая 2012 года в Москве прошел так называемый «Марш миллионов», закончившийся массовыми беспорядками на Болотной площади, в результате которых, согласно официальной информации, пострадали 29 сотрудников полиции. Следственный комитет начал масштабное расследование уголовного дела о массовых беспорядках и случаях насилия в отношении представителей органов правопорядка. Свыше 30 участников протестной акции были осуждены, многие получили реальные сроки, однако полиция не смогла идентифицировать активистов, которые были в масках и капюшонах.

В 2014 году произошел государственный переворот на Украине, к власти в стране пришли противники сближения с Россией. Характерно, что первым импульсом к началу протестов стал пост в Facebook журналиста Мустафы Найема. В целом же социальные сети и Интернет сыграли огромную роль в мобилизации украинцев и координации действий демонстрантов. В частности, через Twitter и Facebook распространялась информация о попытках разгона Майдана, решались различные вопросы (логистика действий, снабжение палаточного лагеря).

Все эти события укрепили убежденность российской власти в опасности как массовых акций в целом, так и использования Интернета для их организации. Примечательно, что уже в 2015 году правительство Москвы развернуло обширную программу по закупке геоаналитики у сотовых операторов.

Необходимо отметить, что даже самая совершенная система отслеживания активности граждан, сочетающая данные об их перемещениях с распознающими лица камерами, не способна остановить по-настоящему массовые выступления. Можно отследить всех, кто писал сообщения в соцсетях или движется в определенную точку сбора, однако, для того чтобы задержать тысячи человек, не хватит ресурса полиции. Тем не менее есть возможность отслеживать активность лидеров протеста, вычислять их местонахождение и задерживать в преддверии уличных акций. Именно такой тактики в последние годы придерживаются правоохранительные органы. Перед большими спланированными акциями задерживают как публичных личностей, так и рядовых активистов. Кроме того, системы слежения и распознавания лиц весьма эффективны для идентификации участников беспорядка и, соответственно, назначения им наказаний в виде арестов и штрафов. Подобные системы эффективны и для составления тематических баз данных и организации политической слежки за лицами, по-

павшими в сферу интересов полиции. В частности, по утверждению ряда оппозиционных активистов, столичные власти устанавливали камеры, подключенные к системе распознавания лиц, на входных рамках во время согласованного митинга на проспекте Сахарова 29 сентября 2019 года. Так же отслеживали участников протестных акций в январе — феврале 2021 года.

С ДРУГОГО БЕРЕГА

Реальность, в которой сегодня существует человечество, такова, что технологические корпорации собирают огромный объем разноплановых данных о пользователях. Правительства развитых стран обрабатывают эти данные[2] с помощью искусственного интеллекта и активно используют для своих нужд, в частности при планировании транспортной или социальной политики. Вопрос, каким образом сохранить приватность и при этом обеспечить безопасность и эффективную работу государственного аппарата, уже много лет находится в центре общественной дискуссии. Особенно она обострилась в 2013 году, когда Эдвард Сноуден раскрыл информацию о государственной программе США PRISM, которая включала в себя массовую слежку за американцами и иностранными гражданами, в том числе через Интернет. В частности, она позволяла Агентству национальной безопасности (АНБ) США просматривать электронную почту, видео и фото, прослушивать голосовые сообщения, отслеживать пересылаемые файлы, собирать информацию из социальных сетей.

С тех пор многие страны приняли дополнительные законодательные меры по защите персональных данных, однако, как показывают исследования Cisco, Pew Research Center, Salesforce, а также других компаний и аналитических центров, люди в среднем имеют весьма смутное представление о том, какие именно данные у них собирают и как они потом используются. При этом абсолютное большинство пользователей всерьез обеспокоены этим вопросом, и их опасения не безосновательны. Технологии слежения и обработки данных развиваются стремительными темпами, регулирование часто не успевает адаптироваться к этим изменениям. Прозрачность технологий наблюдения во многом зависит от государственных механизмов контроля и надзора, которые не всегда достаточно эффективны. Если говорить о странах ЕС, отдельную проблему составляет необходимость соответствия национальных законов нормам европейского законодательства, зачастую во многом устаревшим.

Согласно сообщениям в СМИ, некоторые страны, такие как США, Россия или Китай, неформально требуют от технологических компаний передавать спецслужбам ключи шифрования, позволяющие получать несанкционированный допуск к системам. В октябре 2020 года альянс «Пять глаз» (Five eyes), в который входят разведывательные службы США, Великобритании, Австралии, Канады и Новой Зеландии, а также присоединившиеся к ним спецслужбы Японии и Индии, обратился к технологическим компаниям с требованием, чтобы они — в целях эффективной борьбы с киберпреступностью — предоставляли правоохранительным органам доступ к зашифрованным данным.

При отсутствии глобальных правил игры каждая страна по-своему определяет баланс между приватностью и безопасностью. В странах, которые дела-

ют выбор в сторону большего контроля, неизбежно возникают риски злоупотребления доступом и полномочиями со стороны спецслужб, например, в плане политической слежки. При этом, несмотря на существующие у людей страхи относительно использования их персональных данных, меры по ужесточению контроля под предлогом борьбы с преступностью и терроризмом остаются электорально популярными даже в западных странах, что во многом развязывает правительствам руки для усиления правоохранительных органов и спецслужб.

КИТАЙ: МЕЖДУ ОРУЭЛЛОМ И КАФКОЙ

Безусловным мировым лидером в области цифрового контроля на сегодняшний день является Китай. В 2014 году Госсовет КНР запустил «Программу создания системы социального кредита» (или «социального доверия»), которая предусматривала построение до 2020 года рейтинга доверия, оценивающего компании и физических лиц по баллам. Чтобы заработать или не потерять баллы, требуется соблюдать закон, в том числе правила дорожного движения, платить налоги, вовремя погашать кредиты и оплачивать коммунальные услуги. Рейтинг оценивает также морально-нравственный облик китайцев: баллы можно приобрести за общественно полезные действия или потерять — например, не убрав за своей собакой.

Для обладателей высокого рейтинга система предусматривает различные социальные и экономические льготы, для тех же, у кого он низкий, вводятся административные санкции и ограничения. Например, их лишают возможности купить билет на самолет или скоростной поезд, отправить детей в частную школу. Они могут столкнуться с трудностями при приеме на работу, ограничениями на платформах и онлайн-сервисах, связанных с правительством. Контролировать поведение граждан в китайских городах помогают самые разветвленные в мире системы распознавания лиц. По некоторым оценкам, они охватывают почти все население Китая и способны корректно распознать человека начиная с 9-месячного возраста. В феврале 2020 года публике была представлена обновленная технология, способная распознавать лица, скрытые медицинской маской. В случае подключения камеры к датчику температуры она также может вычислять потенциальных больных, что особенно актуально в период пандемии. Кроме того, начиная с декабря 2019 года пользователи обязаны просканировать свои лица для подключения новых мобильных сервисов или покупки SIM-карты.

Согласно распространенному мнению, внедрение социального рейтинга позволило руководству КНР значительно усилить контроль над обществом. Часто можно видеть публикации, где система демонизируется и сравнивается с реалиями романа Джорджа Оруэлла «1984». Подобным образом охарактеризовал ее, например, бывший вице-президент США Майк Пенс. Согласно другим оценкам, система социального рейтинга крайне неоднородна и не обеспечивает полноценного контроля правительства над обществом. Ее даже называют кафкианской. Вместо сложных алгоритмов с использованием искусственного интеллекта, анализирующего поведение граждан в Сети, есть два списка, «красный» (для «отличников») и «черный» (для «двоечников»), которые открыто публикуются на государственном сайте.

Система нацелена скорее на регулирование самими гражданами своего поведения. Черный список выступает чем-то вроде стенгазеты или «доски позора», попасть на которую стыдно. Разумеется, для жестких нарушителей предусмотрены наказания. Но аналогичные системы используются и в других странах. К примеру, в черном списке Федеральной службы судебных приставов (ФССП России), ограничивающем возможность выезда за рубеж, на конец декабря 2020 года состояли 4,1 млн человек, или почти 3% российского населения. Для сравнения: в Китае по состоянию на март 2019 года в черном списке насчитывалось 13,5 млн человек, или менее 1% населения.

По-настоящему жесткую систему общественного контроля китайское правительство развернуло в Синьцзян-Уйгурском автономном районе (СУАР). Под предлогом борьбы с терроризмом и сепаратизмом власти ввели жесткие ограничения в отношении уйгурского населения региона. Они включают в себя и методы цифрового контроля: все перемещения по СУАР фиксируются камерами, подключенными к системе распознавания лиц и автомобильных номеров. На машины, зарегистрированные в регионе, устанавливаются датчики геолокации. Кроме того, сотни тысяч граждан, по разным причинам признанных не вполне благонадежными, находятся под постоянным наблюдением. Согласно информации в СМИ, система видеослежения сообщает властям о каждом случае, когда они отходят более чем на 300 метров от «безопасной зоны», такой как дом или рабочее место. При этом список подозрительных лиц как минимум частично составляется системой IJOP — искусственным интеллектом для сбора и обработки больших данных о гражданах. Часть помеченных системой людей полиция задерживает и направляет в специальные образовательные лагеря.

В Синьцзяне проводят массовый сбор биометрической информации, сканируют данные мобильных телефонов. Специальное приложение Fengcai, анализирующее данные и трафик, устанавливается даже на смартфоны туристов и журналистов, посещающих регион. При этом вся информация об особенностях режима жесткого цифрового контроля в СУАР поступает преимущественно от представителей СМИ и западных правозащитных организаций. Власти Китая отрицают и тотальную слежку за местными жителями, и наличие лагерей.

Систему распознавания лиц, совмещенную с геоданными, правоохранительные органы активно используют и в других регионах Китая. С ее помощью полиция достаточно эффективно и быстро находит преступников, даже если они успели переместиться в другой город. Не менее развита политическая слежка за оппозиционными и религиозными активистами. В период пандемии технологии слежения помогли Китаю весьма успешно подавить распространение коронавируса. Помимо камер и информации от сотовых операторов власти использовали дроны, данные интернет-магазинов, датчики температуры и огромный спектр технологий на основе искусственного интеллекта для анализа данных о перемещениях и контактах заболевших и потенциально зараженных людей. В известной степени можно говорить о том, что общепризнанный успех Китая в борьбе с пандемией отчасти реабилитировал негативный образ страны, активно применяющей технологии слежения.

ЕВРАЗИЯ — ЦИФРОВОЕ МНОГООБРАЗИЕ

Многие страны Евразии имеют развитые системы распознавания лиц и отслеживания перемещений граждан. Так же, как Россия и Китай, они активно использовали их в борьбе с распространением коронавируса. Среди них — Южная Корея (Республика Корея), продемонстрировавшая, пожалуй, наиболее впечатляющие в мировом масштабе результаты борьбы с пандемией. Правительство следило за действиями граждан, используя геоданные мобильных телефонов (все SIM-карты зарегистрированы и привязаны к владельцам), данные о платежах пластиковыми картами и миллионы камер слежения. При этом большая роль в южнокорейской стратегии противодействия COVID-19 отводилась сознательности граждан. Правительство взяло курс на максимальную открытость — информацию о перемещениях инфицированных лиц моментально публиковали и распространяли органы местного самоуправления через СМИ, СМС и Интернет, в том числе специальные приложения. Таким образом люди могли вовремя узнать о потенциально опасных локациях и избежать их. При этом свобода передвижения граждан не ограничивалась.

Цифровой контроль в Республике Корея имеет давнюю историю, что связано, в частности, с замороженным конфликтом между Сеулом и Пхеньяном. Власти систематически блокируют сайты с северокорейской пропагандой или неподобающим контентом (например, призывами к насилию). В 2015 году был принят закон, обязывающий устанавливать на смартфоны подростков специальное приложение с функциями слежения, с тем чтобы блокировать молодым людям доступ к нежелательной информации. Правоохранительные органы контролируют действия граждан с помощью обширного инструментария. В то же время южнокорейское общество остро реагирует на злоупотребления инструментами слежки со стороны властей. В 2018 году разгорелся большой политический скандал: администрации действующего президента предъявили обвинение в незаконной слежке. В офисе руководителя страны прошли обыски. Ранее, в 2010 году, такие же обвинения едва не стали южнокорейским Уотергейтом для администрации президента Ли Мён Бака.

Технологии помогли также справиться с пандемией Тайваню и Сингапуру. Обоим государствам удалось остановить распространение инфекции на ранней стадии. Сингапур давно использует геоаналитику и камеры распознавания лиц для охраны общественного порядка. Еще в 2014 году правительство запустило масштабную программу цифровизации Smart Nation. В связи с пандемией власти города-государства также внедрили специальное приложение TraceTogether для отслеживания контактов граждан. При этом в начале 2021 года стало известно, что собранные приложением данные доступны полиции и используются для расследования преступлений. К аналогичным мерам цифрового контроля прибег и Тайвань, причем, благодаря эффективному использованию систем слежения и больших данных, стране удалось избежать общенационального карантина. В отличие от Сингапура тайваньское правительство утверждает, что все собранные данные будут уничтожены. Однако в обществе остается тревога по поводу возможности их нецелевого использования.

Другой страной, активно использующей технологии слежения для борьбы с коронавирусом, стала

Индия. Но успеха Южной Кореи ей предсказуемо повторить не удалось. По состоянию на январь 2021 года в Индии насчитывалось свыше 10 млн зараженных, и по этому показателю она занимала второе место в мире после США. Среди причин сложившейся в Индии ситуации с коронавирусом — несравнимая с Южной Кореей численность населения, невозможность длительного локдауна по экономическим причинам и не слишком дисциплинированное поведение граждан. Сыграла свою роль и неготовность технологической инфраструктуры жестко контролировать соблюдение самоизоляции.

Хотя индийские города входят в число лидеров по количеству установленных камер, в стране еще не полностью сформирована единая база изображений. Кроме того, далеко не все камеры подключены к системе распознавания лиц, что делает ее эффективность ограниченной. Так, согласно некоторым оценкам, в период тестирования системы в 2019 году, когда полиция с ее помощью идентифицировала потерявшихся детей, она успешно справлялась с поставленной задачей лишь в 1% случаев. Зачастую камеры не могли корректно определить даже пол ребенка.

В то же время уже в ближайшем будущем это положение может радикальным образом измениться. В конце 2019 года правительство инициировало создание национальной автоматической системы распознавания лиц. Она призвана помочь полиции, испытывающей острую нехватку кадров (в Индии на 100 тыс. населения приходится всего 144 полицейских). В некоторых штатах, таких как Дели и Телингана, уже частично применяются подобные системы. В феврале 2020 года полиция использовала этот инструмент, чтобы опознать 1100 участников межрелигиозных беспорядков на северо-востоке Дели. Согласно сообщениям в СМИ, полиция также применяла камеры, подключенные к системе, во время политических протестов. Некоторые правозащитники утверждают, что создание системы распознавания лиц противоречит индийскому законодательству.

Постсоветские страны Евразии, за исключением России (если быть точнее — Москвы), пока отстают в деле внедрения цифровой слежки. Внутри Центральной Азии система распознавания лиц впервые была установлена в Бишкеке. В марте 2019 года правительство Киргизии подписало с китайской госкомпанией China National Electronic Import and Export Corporation (CEIEC) соглашение о внедрении технологии для укрепления общественного правопорядка и усиления безопасности дорожного движения[3]. В том же году был создан цифровой командный центр ГУВД и установлено 60 камер. В конце 2020 года киргизское руководство объявило о планах установить еще 70 устройств. Внедрение технологий слежения в столице Киргизии вызвало обеспокоенность правозащитников, однако камеры слежения не помешали оппозиции свергнуть президента Сооронбая Жээнбекова в октябре 2020 года.

В июне 2019 года был подписан учредительный договор о создании узбекско-китайского совместного предприятия в рамках проекта «Безопасный город». Его учредителями стали китайские компании CITIC Group и COSTAR Group, а также Центр оказания содействия общественному порядку «Безопасный город» при Министерстве по развитию информационных технологий и коммуникаций Узбекистана. Китайские компании намерены инвестировать в проект 300 млн долларов

с перспективой увеличения объема финансирования до 1 млрд. Планируется внедрение системы распознавания лиц Huawei сначала в Ташкенте, а впоследствии по всему Узбекистану. Масштаб проекта пока до конца не ясен, однако известно, что в 2020 году планировалось завершить создание его единой технологической платформы. Пилотный проект реализуется в Шайхантахурском районе Ташкента, где установлено 898 интеллектуальных камер — впрочем, неизвестно, в каком объеме система функционирует сейчас.

В 2019 году сообщалось также о планах внедрить систему Huawei в Таджикистане, но дальнейшая судьба проекта пока неизвестна. Нет информации и о том, насколько широко применяется в Туркменистане система распознавания лиц, о которой писали оппозиционные издания. Учитывая низкий уровень развития туркменских интернет-технологий и мобильной связи (даже на фоне соседей Туркменистана), остается вопрос, реально ли установить в этой стране эффективную систему цифрового контроля.

В январе 2020 года в ряде изданий вышли публикации о планах по внедрению системы распознавания лиц в крупнейшем мегаполисе Казахстана Алма-Ате. Впоследствии полиция города это опровергла, заявив, что в действительности была проведена лишь презентация технологии местной компании Qamqor. Тем не менее президент страны Касым-Жомарт Токаев в сентябре 2019 года посетил офис китайской компании Hikvision, которая занимается технологиями распознавания лиц и обработки данных. После этого он публично призвал перенять опыт КНР и внедрить аналогичную систему в Казахстане.

ЗАКЛЮЧЕНИЕ

Пандемия предоставила правительствам удобную возможность отработать, что называется, в полевых условиях цифровые технологии, контролирующие население. Страх перед вирусом практически свел на нет фактор общественного сопротивления. То, что еще вчера казалось непозволительным проникновением в частную жизнь, сегодня многими воспринимается как средство спасения.

Даже если власти удалят собранные ими персональные данные, можно с уверенностью утверждать: испытанные в ходе пандемии средства контроля никуда не исчезнут. Их будут применять уже в других целях — от борьбы с преступностью до слежки за «неблагонадежными» лицами и политическими оппонентами. Цифровые технологии использовались для этого и раньше, теперь же масштаб их внедрения, вероятнее всего, значительно возрастет. Показателен пример Москвы, где после признанного успешным опыта борьбы с пандемией планируется расширить сеть камер с распознаванием лиц.

Сегодня технологии не позволяют осуществлять стопроцентный тоталитарный контроль в больших масштабах. Китайская практика управления Синьцзян-Уйгурским автономным районом скорее исключение, чем правило. Цифровой контроль не способен также остановить по-настоящему массовые общественные выступления: задерживают людей по-прежнему не камеры, а сотрудники полиции. Тем не менее, как показывает опыт России, Китая, Индии, Республики Корея и многих других государств, существующего инструментария вполне достаточно для слежки и нейтрализации конкретных политиков и активистов. Человек может

не замечать существующей в его городе или стране системы до тех пор, пока он сам не окажется в фокусе ее внимания.

Пандемия значительно сместила баланс между неприкосновенностью частной жизни и безопасностью (понимаемой в каждой стране по-своему) в пользу последней. Когда шок от эпидемии пройдет, постковидным обществам придется искать новые механизмы, чтобы сдержать стремление властей к повсеместному цифровому контролю.

Статья опубликована в рамках проекта «Диалог Россия — США: смена поколений». Взгляды, изложенные в статье, отражают личное мнение автора.

ПРИМЕЧАНИЯ

1 Статья 207.1 Уголовного кодекса РФ «Публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан» вступила в силу 1 апреля 2020 года.

2 Официально сообщается, что они обезличенные, однако, как уже было сказано, определить с их помощью личность человека не составляет большого труда.

3 Интересно, что CEIEC предоставила Киргизии эту технологию бесплатно. См.: https://informburo.kz/stati/kak-ustroeny-sistemy-raspoznavaniya-lic-i-nado-li-ih-opasatsya-.html

ОБ АВТОРЕ

Николай Маркоткин — эксперт Российского совета по международным делам.

МОСКОВСКИЙ ЦЕНТР КАРНЕГИ