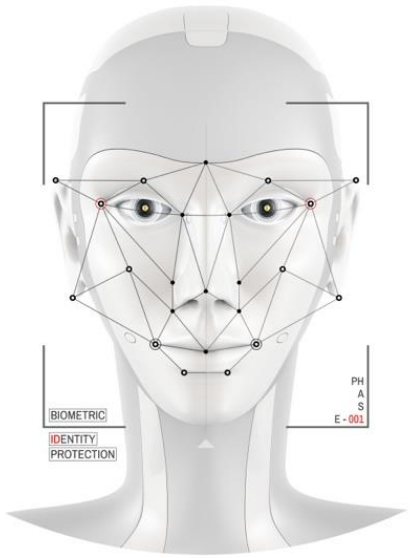
Распознавание лиц: предчувствие антиутопии

Настоящий доклад подготовлен экспертами проекта «Сетевые Свободы» и посвящен исследованию проникновения технологии facial recognition в жизнь россиян. В некоторой степени он продолжает серию докладов «Россия под наблюдением», в которых анализировалось развитие различных технологий массовой слежки и их влияние на права и свободы. Мы планируем описать ситуации, в которых обычный гражданин может столкнуться с распознаванием лиц, а также существующее нормативное регулирование этой сферы.



Распознавание лиц (facial recognition, FR) — метод компьютерной идентификации или подтверждения личности по цифровому образу. Для этого система выделяет отличительные детали лица человека, как правило — расстояние между глазами, глубину глазниц, расстояние от лба до подбородка, размер и форму подбородка, скул, губ, ушей и т.п. Эта информация затем преобразуется в математический вид, а полученный таким образом

«отпечаток лица» уже можно сравнивать с данными об изображениях, имеющихся в базе.

Конкретные алгоритмы и точность работы различных систем FR могут различаться: эффективность распознавания зависит от разрешения камеры, степени освещенности, угла обзора, доступности лица и других подобных факторов. Некоторые их них вместо точной идентификации человека оценивают совпадение изображения с имеющимися в базе цифровыми отпечатками лиц, ранжируя их по степени вероятности.

Появившаяся несколько десятилетий назад технология идентификации лиц по изображениям с развитием вычислительной мощности компьютеров и видеоаналитики открыла совершенно новые возможности как для повышения комфорта и улучшения безопасности, так и для тотального контроля со стороны правительств и корпораций.

Два года назад во время слушаний в Комитете Палаты представителей США стало известно, что ФБР имеет в своем распоряжении постоянно увеличивающуюся базу из 640 миллионов фотографий (среди которых, к примеру, фото из водительских удостоверений, выданных в 21 штате).

Сегодня распознавание лиц используется для разблокировки смартфонов, авторизации в приложениях, организации цифровых фотоальбомов, оплаты проезда в общественном транспорте, установления личности при обращении за государственными или банковскими услугами, пересечения границ, организации пропускного режима на предприятиях, расследования преступлений, поиска пропавших граждан. В то же время с помощью алгоритмов нейронных сетей власти разных стран контролируют перемещения горожан, следят за мирными протестующими и преследуют дискриминируемые меньшинства. Общедоступные сервисы, предлагающие услуги поиска профилей в социальных сетях по изображениям, используются для деанонимизации и травли, растет рынок «пробива» по камерам городского видеонаблюдения.

В целом технология настолько эффективна, что ее массовое распространение в отсутствие столь же эффективных и

прозрачных механизмов защиты общественных интересов и гарантий соблюдения прав граждан несет серьезную угрозу. Риски утечек, злоупотреблений со стороны тех, кто имеет доступ к камерам, использования технологии для массовой слежки, дискриминации и выявления «политически неблагонадежных» лиц, а также ошибок распознавания настолько велики, что в ряде стран всерьез обсуждается полный или частичный запрет распознавания лиц без согласия граждан, в отношении которых оно может применяться.

В России с инициативой введения временного моратория на использование систем распознавания лиц до тех пор, пока не будет обеспечена полная прозрачность и безопасность их использования для граждан, выступает Роскомсвобода.

Распространение facial recognition в России можно условно разделить на три этапа: подготовка (с 2001 по 2015 год происходила установка камер и создавались первые программные комплексы), тестирование (с 2016 по 2018 год технология активно апробировалась в рамках развития городских программ общественной безопасности и подготовки к проведению международных спортивных соревнований) и широкое внедрение (с 2019 по настоящее время продолжается унификация протоколов и интеграция разрозненных сетей в единое пространство)*.

Распространение технологии

Впервые о массовом применении технологии в России заговорили на рубеже прошлого десятилетия в связи с двумя событиями: повсеместной установкой камер видеонаблюдения и появлением сервисов поиска людей по фотографии.

Огромный массив изображений как для верификации, так и для обучения алгоритмов дают социальные сети, куда пользователи добровольно загружают гигабайты собственных фотографий.

В 2016 году на рынок вышли сразу несколько веб-сервисов, предлагающих за небольшую плату поиск пользователей «ВКонтакте» по фотографии (к примеру, за 5 евро можно было не

* Хронологию внедрения технологии FR в России можно увидеть здесь.

только получить возможность отправлять до 300 запросов в месяц, но и удалить собственную личность из результатов выдачи). К этому времени Россия уже несколько лет активно покрывалась сетью камер высокого разрешения. Объединение двух систем сулило колоссальные преимущества.

Системы городского видеонаблюдения начали появляться в Москве в 2001 году. Это были маломощные черно-белые камеры, установленные в подъездах жилых домов (около 80 тысяч камер) и общественных местах (120 камер). В то время они еще не были объединены в общую сеть, а разобрать лица людей на них было невозможно. Изображения с камер поступали в 125 локальных центров мониторинга.

К 2005 году отдельные группы камер начали подключать к Пунктам центрального видеонаблюдения, создававшимся в каждом районе города и требовавшим постоянного участия человека. В 2007 году система была впервые модернизирована в рамках только появившейся тогда еще городской программы «Безопасный город».

В 2011 году началась полноценная реформа системы городского наблюдения — в Москве появился Единый центр хранения и обработки данных с возможностью удаленного доступа к изображениям с камер в режиме реального времени, а также архиву записей. В то же время появились первые сообщения о внедрении технологии распознавания лиц в систему видеонаблюдения на транспорте, которая, впрочем, массового применения тогда не получила.

Стоит отметить, что как раз в 2011 году в России возобновился рост протестной активности — митинги против фальсификации результатов парламентских, а позднее и президентских выборов собирали десятки тысяч человек.

Летом 2012 года по всей Москве установили уже 60 тысяч новых камер. Тогда же участникам протестов запретили скрывать лица, в том числе использовать маски, средства маскировки и прочие подобные приспособления, затрудняющие установление личности.

В 2014 году началось создание региональных программ обеспечения безопасности, а также установка и расширение

систем городского видеонаблюдения в ряде регионов — Республике Коми, Астраханской, Свердловской и Томской областях, Санкт-Петербурге и др.

В Москве Ростелеком начал подключение более 60 тысяч современных городских камер к Единому центру хранения и обработки данных. При этом уже тогда расследование правонарушений в городе в 70% случаев осуществлялось с использованием данных системы видеонаблюдения.

В этом же году по поручению Владимира Путина началось масштабирование «Безопасного города» на всю страну: была утверждена Концепция построения и развития АПК «Безопасный город» (АПК БГ), а также создана Межведомственная комиссия по ее внедрению. Ключевой особенностью нового комплекса стала интеграция на единой платформе информационных и телекоммуникационных систем, отвечающей за безопасность транспортной инфраструктуры, полицейских баз данных, информационных систем Минздрава, МЧС, органов управления ЖХК, региональных, районных и муниципальных структур. Началось объединение ранее созданных и подтвердивших свою перспективность систем безопасности для обеспечения сквозной передачи и обработки всего массива данных с разграничением уровней доступа.

В Концепции констатировалось наличие разнообразных угроз природного, техногенного, биолого-социального, экологического и другого характера, в том числе — ураганы, землетрясения, наводнения, различные аварии, эпидемии, действия организованной преступности, падение крупных небесных тел, несанкционированные публичные мероприятия и массовые беспорядки. В реализации программы задействованы как минимум 18 различных ведомств: от МВД, ФСБ, ФСО и Росфинмониторинга до Минспорта и Федерального космического агентства.

Обеспечивать безопасность АПК БГ должен с помощью организации видеонаблюдения и видеоаналитики в реальном времени, позиционирования подвижных объектов, акустического мониторинга (фиксации криков, ударов, хлопков, выстрелов, боя стекла), геолокации объектов, отслеживания маршрутов всех видов транспортных средств, прогнозирования и восстановления

хронологии происшествий, хранения данных, а также (внимание!) **идентификации и распознавания лиц**.

В 2015 году (подготовка к Кубку Конфедераций — 2017 и Чемпионату мира по футболу — 2018 была в самом разгаре) Правительство утвердило требования к антитеррористической защищенности мест массового пребывания людей и спортивных объектов. Согласно постановлениям, все места массового пребывания людей (то есть такие, в которых могут собраться более 50 человек) должны быть оборудованы системами непрерывного видеонаблюдения, обеспечивающими архивирование и хранение данных в течение 30 дней. Спортивные объекты, на которых в результате террористической атаки могут пострадать более 500 человек, должны быть дополнительно оснащены системами видеонаблюдения с функцией идентификации посетителей.

Эти технологии используются также для выявления футбольных фанатов, состоящих на учете МВД. Системами распознавания лиц оборудуют в первую очередь фанатские секторы и турникеты на входе. К примеру, АПК «Визирь» от компании ЦРТ, установленный на 16 крупнейших стадионах и ледовых аренах страны, обеспечивает (по утверждению разработчиков) видеоконтроль доступа и идентификацию посетителей при проходе через турникеты, посещении касс, регистрации и оформлении входных документов, предоставляет возможность сбора фотографий болельщиков, передачу их в CRM-систему клуба и ведение картотеки, связанной с информационными системами МВД и РПЛ.

Лидером видеонаблюдения и полигоном для отработки технологии видеоаналитики стала Москва. К 2016 году в городе уже было установлено почти 130 тысяч камер видеонаблюдения — на дорогах, в подъездах многоквартирных домов, во дворах, муниципальных объектах и супермаркетах. Оставалось только прикрутить к этой сети программное обеспечение, которое идентифицировало бы объекты и лица.

18 февраля 2016 года никому не известная в то время компания NtechLab, основанная 26-летним выпускником Московского университета Артемом Кухаренко, официально представила приложение FindFace — веб-сервис, предлагающий искать людей в социальной сети «ВКонтакте» по их фотографиям. В мае 2016

года число посетителей сервиса достигло 1 млн человек, месячная аудитория «ВКонтакте» к тому времени превысила 46 миллионов пользователей — вполне достаточная база для обучения нейросети. Спустя год стало известно о сотрудничестве компании с московским Департаментом информационных технологий — первые три тысячи камер были подключены к системе осенью 2017 года, доступ к ним получили 16 тысяч человек — силовики, а также представители государственных и муниципальных организаций.

Кухаренко в интервью говорил, что FindFace — лишь способ презентовать технологию. Идея сработала: об NtechLab заговорили, причем в контексте «конца частной жизни» и «уничтожения приватности». Вскоре после этого компания прекратила поддержку сервиса для широкой публики, сосредоточившись на оказании услуг корпорациям и государству.

Московские власти сообщали, что уже на стадии испытаний системы в городских условиях она позволила выявлять правонарушителей — в течение первых двух месяцев с ее помощью задержали шестерых человек, находившихся в розыске.

Одновременно перспективную технологию начали тестировать и на участниках акций протеста. 12 июня 2017 года по всей стране прошли митинги против коррупции. В Москве согласованный с городскими властями митинг был запланирован на проспекте Сахарова. Накануне государственные агентства распространили заявление, что металлодетекторы на входе в место проведения акции будут оснащены камерами с функцией распознавания лиц.

В следующие два года эксперименты продолжились: ДИТ Москвы использовал систему на 17 массовых мероприятиях, а в 2019 году МВД сообщило, что за прошедшее время она помогла выявить и задержать 90 человек, находившихся в розыске (в московском метро, которое подключили к распознаванию лиц в 2018 году, ежемесячно задерживали от 5 до 10 человек).

В 2018 году NtechLab поставила свою систему МВД по Рязанской области, которое начало использовать ее на массовых мероприятиях, устанавливая камеры на металлодетекторы и подвижные наблюдательные пункты на базе полицейских автомобилей; запустила сеть из 25 камер в Альметьевске;

внедрила систему обезличенной видеоаналитики в одном из торговых центров Санкт-Петербурга.

Во время ЧМ-2018 система FindFace Security, подключенная к 500 камерам на стадионах, принимавших матчи турнира, позволила задержать 180 правонарушителей. К этому времени 12,5%+1 акцией компании владел Ростех, планировавший развивать систему «умных городов» с фокусом на общественную безопасность.

В настоящее время компания предлагает многофункциональные биометрические решения проблем безопасности государства и бизнеса. В рекламном проспекте говорится, что софт способен в режиме реального времени определять лица в видеопотоке и считать людей, сверять полученные данные со списками мониторинга, уведомлять пользователя при обнаружении совпадений и предоставлять наглядные статистические отчеты. Он может быть интегрирован в системы управления доступом, кассовые аппараты и другие сторонние сервисы. При этом идентификация с точностью 99% по базе из 1,5 млрд лиц занимает менее 1 секунды.

Более того, программа агрегирует информацию о действиях людей, в разное время попадавших в поле зрения камер, создавая профайл, который может быть использован как в полицейских, так и в коммерческих целях («теперь можно узнать клиента, как только он зашёл в магазин, проанализировать его прошлые покупки и предложить релевантные товары»), а также для построения карты контактов — каждое лицо проверятся на наличие контактов с другими лицами, которые попадали в кадр камеры наблюдения.

В марте 2020 систему видеоаналитики от ЦРТ, которую первоначально устанавливали на стадионах, адаптировали к поиску и выявлению больных COVID-19 и контактных лиц. Подобные решения также предлагают NtechLab и VisionLabs. Пандемия в целом дала мощный толчок развитию различных технологий слежки, в том числе — с использованием распознавания лиц.

К 2020 году АПК «Безопасный город» действовал в 40 регионах, во многих из них — с использованием FR, в том числе в Москве и

Московской области, Санкт-Петербурге, Рязанской, Саратовской, Нижегородской, Челябинской, Тюменской, Кемеровской областях, ХМАО, Камчатском и Приморском краях, а также в Крыму.

Судя по всему, на очереди объединение разрозненных региональных комплексов в единую систему: правительственный Институт законодательства и сравнительного правоведения разработал проект федерального закона «О единой системе «Безопасный город»*.

Жителей Москвы привлекали к ответственности за нарушение карантина на основании информации, полученной с подъездных камер. На Сахалине возможная ошибка системы распознавания лиц не помешала оштрафовать жительницу Томска за несоблюдение карантинных мер. Однако — помимо собственно контроля за соблюдением противоэпидемических мер — у создателей был на руках крайне убедительный в условиях пандемии аргумент в пользу широкого внедрения автоматизированных биометрических систем — их использование позволяет сократить количество непосредственных контактов между людьми, то есть также уменьшает риск распространения инфекции.

Крупные банки инициативно начали внедрять технологии биометрической идентификации клиентов — в том числе с использованием технологии распознавания лиц. Летом 2020 года Альфа-Банк открыл в Москве первое отделение, в котором клиентов идентифицируют по биометрическим данным: «клиенту достаточно войти в офис, и система передаст сотруднику всю важную информацию: как зовут клиента, какими сервисами банка пользуется, с какой проблемой пришел, что ему может быть интересно». Сбербанк уже предлагает подключить распознавание по лицу онлайн.

Параллельно создается федеральный банк биометрических данных: Единая биометрическая система (совместный проект Банка России и Ростелекома) получила статус государственной информационной системы, а все собранные с ее помощью персональные данные должны быть интегрированы с Единой

* Карту использования технологии FR можно увидеть здесь.

системой идентификации и авторизации (ЕСИА), дающей доступ к государственным услугам.

Весной 2021 года Правительство разрешило вузам проводить промежуточную аттестацию дистанционно с использованием Единой биометрической системы.

Отдельного внимания заслуживает использование видеонаблюдения и распознавания лиц для выявления участников несанкционированных протестов. Систематическое использование фото- и видеодоказательств отмечалось еще во время «Болотного дела». Причем в то время значительный массив записей был получен от журналистов, снимавших протесты. Вероятно, в 2012-2015 годах собственного видео было недостаточно.

С тех пор объем и качество видеоматериалов постоянно росли, и в «Московском деле» уже имелось большое количество высококачественной полицейской съемки, в том числе с камер, носимых сотрудниками в штатском, что позволяло увеличивать картинку без значимой потери качества, получая крупные планы.

Полиция явно собирает картотеку участников протестов, что подтверждается массовым фотографированием задержанных, о котором сообщали адвокаты и активисты из Санкт-Петербурга, Москвы Самары и Казани.

Однако в материалах дел об административных правонарушениях следов использования автоматического распознавания лиц нет, при этом медиа явно создают видимость ее массового применения, что позволяет выдвинуть ряд гипотез:

— имеющиеся в распоряжении властей технологии пока несовершенны и не позволяют в автоматическом режиме генерировать доказательства, либо труд рядового полицейского дешев, а установка оборудования и программного обеспечения пока дорога;

— власти тестируют и хотят внедрить распознавание лиц как можно шире и при этом как можно дольше не вводить нормативное регулирование, которое неизбежно ее ограничит;

— доказательства применения не афишируются, чтобы не создавать оснований для судебных разбирательств, способных

публично поставить под сомнение правомерность ее использования.

Регулирование

А. Международные нормы

Автоматическое распознавание лиц — сравнительно новая технология, а потому международным правом напрямую не урегулированная. Однако уже существующие договоры устанавливают общие критерии, которым она в любом случае должна соответствовать.

1. Документы ООН

В 2020 году Комитет по правам человека, созданный на основании ст.40 Международного пакта о гражданских и политических правах, принял Замечания общего порядка №37 по статье 21 Пакта о праве на свободу собраний. Поскольку Замечания отражают современное представление о содержании того или иного права, Комитет высказался и о распознавании лиц, отметив связь свободы собраний с правом на неприкосновенность частной жизни, и указав, что эти права могут быть нарушены, например, с помощью распознавания лиц и других технологий, позволяющих идентифицировать отдельных участников в толпе. То же самое относится и к мониторингу социальных сетей для сбора информации об участии в мирных собраниях.

2. Документы Совета Европы

Базовым документом, регулирующим в том числе и использование технологии распознавания лиц, является Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных 1981 года (Конвенция 108), которую Россия ратифицировала в 2013 году. С тех пор был принят Протокол, которым Конвенция 108 была серьезно обновлена, чтобы соответствовать требованиям времени (так называемая Конвенция 108+), однако Протокол Россия до сих пор не ратифицировала, хотя и подписала в 2018 году.

Тем не менее даже в исходном тексте 1981 года достаточно норм, позволяющих оценивать автоматическое распознавание лиц. Конвенция 108 начинает с того, что определяет «персональные данные» как любую информацию об определенном или поддающемся определению физическом лице. Статья 6 Конвенции 108 предусматривает, что персональные данные, касающиеся расовой принадлежности, политических взглядов или религиозных или других убеждений, а также здоровья или половой жизни (так называемые «чувствительные персональные данные»), не могут подвергаться автоматизированной обработке, если внутреннее законодательство не устанавливает соответствующих гарантий.

Основные принципы обработки персональных данных (ст.5) требуют гарантировать, что они:

a) собираются и обрабатываются на справедливой и законной основе;

b) хранятся для определенных и законных целей и не используются иным образом, несовместимым с этими целями;

c) являются адекватными, относящимися к делу и не чрезмерными для целей их хранения;

d) являются точными и, когда это необходимо, обновляются;

e) сохраняются в форме, позволяющей идентифицировать субъекты данных не дольше, чем это требуется для целей хранения этих данных.

Конвенция 108 предусматривает ряд прав для граждан, чьи персональные данные обрабатываются — прежде всего, права знать об обработке, получить доступ к данным, просить внести в них изменения или удалить.

Конвенция 108 предусматривает создание Консультативного комитета государств-участников (Комитет 108), который может высказываться по вопросам применения Конвенции. Комитет 108 принял серьезный объем документов, которые раскрывают положения Конвенции, адаптируют их к требованиям времени.

Так, 28 января 2021 года Комитет 108 принял Руководящие принципы по распознаванию лиц. Согласно документу,

биометрические данные относятся к категории особо чувствительной информации, а их обработка признается потенциально угрожающей частной жизни.

Не без одобрения упоминая общий запрет автоматического распознавания лиц по GDPR (о нем ниже), Руководящие принципы начинают описание регулирования с вопросов, которые должно урегулировать национальное законодательство в отношении использования распознавания лиц в каждой сфере:

— детальное объяснение использования технологии и ее целей;

— минимальные требования к точности и надежности алгоритма;

— срок хранения полученных изображений;

— возможность проверки соблюдения (аудита) этих требований;

— «прослеживаемость» процесса применения технологии;

— защитные механизмы.

Использование автоматического распознавания лиц в общественных местах — от школ до торговых центров — по мнению Комитета 108, должно быть предметом демократического общественного обсуждения и не может применяться до завершения оценок пропорциональности ограничения прав и свобод человека.

Специально должны быть урегулированы процедуры получения образцов данных о лицах из цифровых изображений. При этом **Комитет 108 отрицательно относится к сбору образцов из фотографий, опубликованных в Интернете, в том числе в социальных сетях, и (или) полученных с камер видеонаблюдения, если законность такого сбора обосновывается лишь тем, что граждане сами предоставили свои изображения**.

В общественном секторе, в отношениях гражданина и государства согласие на использование изображения не может, по мнению Комитета 108, являться основанием для применения распознавания лиц. Но Комитет 108 настаивает на том, что эта технология должна применяться только для целей поддержания правопорядка с соблюдением требований пропорциональности

(для предотвращения и расследования только наиболее тяжких преступлений) и быть детально урегулирована законом. Среди примеров непропорционального использования распознавания лиц Комитет 108 приводит применение этой технологии для якобы обеспечения безопасности школ и других общественных зданий, если существуют альтернативы.

Частному сектору Комитет 108 предлагает применять распознавание лиц исключительно на основе ясного, специфического, информированного и добровольного согласия и после того, как потребителю был предоставлен альтернативный способ идентификации. Специфичность согласия заключается в том, что не допускается использование технологии распознавания лиц для иных целей, чем те, на которые оно дано. Комитет 108 не допускает использование распознавания лиц частными организациями в местах скопления людей типа торговых центров.

Кроме того, Комитет 108 предлагает введение сертификации алгоритмов распознавания лиц и принципы, которые должны соблюдаться при разработке алгоритмов. Требования к операторам данных также подробно излагаются в Руководящих принципах и включают необходимость защиты от утечек, оценку воздействия на защиту данных, защиту данных как часть дизайна и соблюдение этических норм. Среди последних — необходимость проверки (аудита) применения технологии независимыми комиссиями. Права граждан в Руководящих принципах, как и в Конвенции 108, включают право знать причины применения технологии, право возражать против ее применения и право требовать внесение изменений в персональные данные.

Комитет 108 заканчивает Руководящие принципы требованием не принимать решения в отношении граждан исключительно на основании данных распознавания лиц и без участия самих затронутых граждан.

3. Документы Шанхайской организации сотрудничества

Совет Европы — не единственная международная организация с участием России, которая приняла документы о технологии распознавания лиц. Шанхайская организация сотрудничества объединяет Россию, Китай и страны Центральной Азии в сфере

безопасности и противодействия экстремизму, сепаратизму и терроризму. В ее рамках заключено двустороннее соглашение РФ и КНР о сотрудничестве в борьбе с терроризмом, сепаратизмом и экстремизмом. Статья 7 этого соглашения допускает обмен данными между двумя государствами — об организациях, созданных для совершения терроризма, сепаратизма и экстремизма, и **их членах,** по возможности включая названия, структуру и основную деятельность организаций, а также фамилии, сведения о гражданстве, месте жительства или месте нахождения, **характерных чертах внешности, фотографии, отпечатки пальцев и другие сведения об их членах, полезные для определения и опознавания этих лиц.**

То есть Россия и Китай договорились обмениваться результатами применения технологии распознавания лиц, когда они считают, что распознаны лица тех, кого эти два государства считают террористами, сепаратистами или экстремистами. Соглашение не обусловливает обмен данными никакими требованиями законности их сбора, специфичности их использования, пропорциональности и даже срока хранения.

Б. Сравнительное право

1. Европейский Союз

27 апреля 2016 года в Европейском Союзе был принят Генеральный регламент по защите данных 2016/697 (GDPR). Пункт 14 его преамбулы и статья 9 ясно и недвусмысленно запрещают сбор биометрических персональных данных без предварительного согласия субъекта этих данных. Таким образом, автоматическое распознавание лиц без согласия запрещено европейской нормой прямого действия. Попытки создать систему автоматического распознавания лиц, которая бы удовлетворяла Генеральному регламенту, пока успехом не увенчались.

Европейская Комиссия готовит в настоящее время проект директивы по искусственному интеллекту, нормы которой могут регулировать и системы распознавания лиц. При обсуждении проекта директивы Европейский Совет по защите данных и Европейский Комиссар по защите данных опубликовали

совместное заключение, в котором высказались и про эту технологию.

Принимая во внимание чрезвычайно высокие риски, связанные с удаленной биометрической идентификацией людей в общедоступных местах, Совет и Комиссар призывают к общему запрету на любое использование искусственного интеллекта для автоматического распознавания людей в общедоступных местах — таких как распознавание лиц, походки, отпечатков пальцев, ДНК, голоса, нажатия клавиш и других биометрических или поведенческих сигналов в любом контексте. Они также рекомендуют запретить системы искусственного интеллекта, использующие биометрию, для разделения людей на группы по признаку этнической принадлежности, пола, политической или сексуальной ориентации или по другим запрещенным признакам. Кроме того, Совет и Комиссар считают, что использование искусственного интеллекта для определения эмоций человека крайне нежелательно и должно быть запрещено — за исключением очень конкретных случаев (таких как некоторые медицинские цели, для которых важно распознавание эмоций пациента). Кроме того, они пришли к выводу, что использование искусственного интеллекта для любого типа социальных оценок должно быть запрещено.

Заключение Совета и Комиссара касаются как распознавания лиц в общественных местах в реальном времени, так и последующего автоматического распознавания лиц по записям камер наблюдения. Они отдельно высказываются о распознавании лиц в ходе демонстраций политического характера: «Удаленная биометрическая идентификация в контексте политического протеста, вероятно, окажет значительный охлаждающий эффект на осуществление основных прав и свобод — таких как свобода собраний и ассоциаций и в более общем плане основополагающих принципов демократии».

2. Великобритания (Соединенное Королевство)

В Великобритании полиция осуществляла попытки применить автоматическое распознавание лиц. Эти действия привели к судебному делу *Бриджес против Главного констебля Полиции*

Южного Уэльса, в котором валлийский активист требовал признать незаконными поездки по городу полицейского фургона с камерами.

В первой инстанции дело слушалось в Высоком суде в Кардиффе, который признал, что распознавание лиц представляет собой гораздо более серьезное вмешательство в право на неприкосновенность частной жизни, чем система видеонаблюдения CCTV. Высокий суд принял во внимание тот факт, что полиция разыскивала конкретных лиц в определенных списках наблюдения при применении технологии, и это происходит на мероприятиях, которые ранее сопровождались насилием или ложными сообщениями о терактах. Результаты анализировались системным оператором — ложные результаты немедленно удалялись. Высокий суд согласился с тем, что за использованием технологии в достаточной мере осуществляется надзор со стороны консультативного совета и посредством независимого академического анализа. Он пришел к выводу, что использование технологии распознавания лиц соответствует Закону о правах человека (*Human Rights Act*) и Закону о защите данных (*Data Protection Act*).

11 августа 2020 года Апелляционный суд Англии и Уэльса единогласно отменил решение по апелляции г-на Бриджеса. Хотя Апелляционный суд признал существование гарантий, связанных с применением распознавания лиц, он счел принимаемые меры недостаточными. Данные, собранные с помощью этой технологии, признавались «конфиденциальными» в соответствии с Законом о защите данных, тогда как усмотрение, предоставленное сотрудникам полиции, было признано слишком широким. Было также установлено, что технология нарушает обязательство по обеспечению равенства в государственном секторе.

Решение Апелляционного суда является на сегодня наиболее подробным анализом технологии с точки зрения прав человека и защиты персональных данных.

3. США

В отсутствие федерального законодательства и без специального регулирования на уровне штатов около 20 муниципалитетов в США ввели запреты на использование автоматического распознавания

лиц на местном уровне. Это важно, поскольку значительная часть полиции подчиняется в США именно муниципалитетам. В Бостоне и Кэмбридже, штат Массачусетс (кстати, именно там расположены Гарвардский университет и Массачусетский технологический институт), распознавание лиц запрещено в деятельности полиции и всех других местных органов власти. Такой же запрет введен в графстве Кинг в штате Вашингтон, где расположены головные офисы Microsoft и Amazon. В Портленде, Орегон — также растущем технологическом центре — запрет распознавания лиц распространяется не только на деятельность властей, но и на частный бизнес.

На уровне штатов один из наиболее подробных законов о биометрических персональных данных существует в Иллинойсе, он стал основой для исков, оспаривающих применение распознавания лиц. В суде графства Кук, включающем Чикаго, находится на рассмотрении иск ряда правозащитных организаций (в частности, Американского союза гражданских свобод) к компании Clearview, разрабатывающей программное обеспечение для распознавания лиц. Мировым соглашением закончилось дело против Facebook, в котором применялось, в том числе право Иллинойса. Истцы получили компенсацию от социальной сети за предложения пользователям отметить их друзей на фотографиях, поскольку предложения были сгенерированы технологией распознавания лиц, на применение которой пользователи предварительного согласия не давали.

События у Капитолия 6 января 2021 года привели к применению технологии как полицией, так и отдельными энтузиастами с целью распознать участников атаки на здание Конгресса и Сената. В результате как столкновений у Капитолия, так и все большего числа судебных исков был внесен ряд федеральных законопроектов для урегулирования или запрета автоматического распознавания лиц, но пока ни один из них не продвинулся в парламентской процедуре.

B. Российское регулирование

Хотя системы распознавания лиц тестируются и применяются в России уже более 10 лет, почти никаких специальных положений,

регулирующих эту технологию, в российском праве нет. Отдельные элементы урегулированы для отдельных отраслей, но только в банковской сфере можно говорить о достаточно подробной регламентации процесса.

Федеральный закон от 31 декабря 2017 года №482-ФЗ создал основание для создания и введения «единой информационной системы персональных данных, обеспечивающей обработку, включая сбор и хранение, биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации». Это название из четырех строк в самом законодательстве сокращается до «единой биометрической системы». Ее существование определяется статьей 14.1 ФЗ «Об информации, информационных технологиях и защите информации», которая предусматривает сбор данных для хранения в единой биометрической системе и использования их для идентификации граждан. Среди собираемых данных изображение лица упоминается в первую очередь (Постановление Правительства РФ от 30 июня 2018 года №772). Поскольку законодательство прямо признает изображение лица биометрическими персональными данными, логично, что статья 14.1 Закона об информации (как и ст.11 ФЗ «О персональных данных») требует личного присутствия и прямого письменного согласия гражданина на сбор, хранение, обработку и использование изображения его лица.

Банки, которые удовлетворяют определенным критериям (прежде всего — участвуют в системе страхования вкладов), могут открывать и вести счета клиентов-физических лиц, предоставлять кредиты, а также осуществлять переводы денежных средств по таким счетам по их поручению без их личного присутствия, идентифицируя клиентов через биометрию. Интересно, что эти возможности предоставлены банкам не Законом РФ «О банках и банковской деятельности», а Федеральным законом «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма». Подозрения в отмывании денег и финансировании терроризма дают право банкам отказывать в проведении этих операций без личного присутствия клиента.

В отношении деятельности государственных органов Закон об информации и Постановление Правительства РФ от 30 июня 2018 года №772 описывают лишь объем собираемых и хранимых для идентификации гражданина данных, но не определяют ни государственные органы, уполномоченные идентифицировать человека по биометрическим данным, ни ситуации, в которых такая идентификация возможна, ни какие-либо гарантии и ограничения, препятствующие произволу. Пункт 10 статьи 14.1 Закона об информации предусматривает контроль со стороны ФСБ, но он, вероятно, не будет ни прозрачным, ни публичным.

Тем не менее нормы права очевидно относят изображения лица к биометрическим персональным данным, а значит, для их сбора и использования требуется предварительное согласие. Эти законы ставят препятствия для широкого использования системы распознавания лиц. Пытаясь избежать соблюдения этих норм, компании, предлагающие услуги распознавания, в рекламных проспектах подчеркивают, что обрабатываемые данные сами по себе не являются персональными — не связаны с информацией о личности, а цифровые отпечатки лиц не позволяют воссоздать исходное изображение. На статью 14.1 Закона об информации и статью 11 Закона о персональных данных нет ссылок и в судебных делах, где оспаривалось распознавание лиц в Москве.

Два дела касались протестов. Это одиночный пикет Алены Поповой около здания Государственной Думы, а также демонстрация на проспекте Сахарова 29 сентября 2019 года против репрессий, связанных с предвыборной кампанией в Московскую городскую думу. За первое мероприятие Попову оштрафовали на основании данных системы распознавания лиц. Что касается второго мероприятия, то на входе на проспект Сахарова на уровне головы человека среднего роста стояли камеры, что свидетельствовало о фотографировании всех участников политического оппозиционного митинга. В обоих случаях Департамент информационных технологий Правительства Москвы не отрицал применение технологий распознавания лиц, а в случае митинга 29 сентября 2019 года даже представил документ МВД о ее применении. В третьем деле истица купила записи с камер распознавания лиц с данными о себе на «черном рынке».

Во всех трех делах московские власти утверждали (а суды с ними согласились), что при использовании технологии распознавания лиц не применяются не только законодательные положения о персональных данных, но и вообще персональные данные никак не задействованы. Московские власти и суды ссылались на то, что камеры видеонаблюдения снимают открытые пространства — например, улицы и дворы — граждане же не являются основным объектом наблюдения, а потому использование данных людей, попавших в обзор камер наблюдения, возможно без их согласия по статье 152.2 Гражданского кодекса РФ. Использование камер видеонаблюдения и режим хранения и обработки полученной съемки урегулированы Постановлением Правительства Москвы от 7 февраля 2012 года №24-ПП о Едином центре хранения данных, а потому в глазах властей и судов оно законно.

Позиция московских судов, уже поддержанная вышестоящими инстанциями, едва ли в ближайшее время претерпит изменения, а значит, судебная практика идет по пути прямого отказа признавать изображения граждан, собираемые камерами городского видеонаблюдения, биометрическими персональными данными. В отличие, например, от ситуации, когда эти данные используются для идентификации банками и государственными сервисами.

Наконец, федеральный закон №123-ФЗ об эксперименте с искусственным интеллектом в Москве, принятый 24 апреля 2020 года, полностью освобождает московские власти от соблюдения федерального законодательства о персональных данных. Предоставляя мэрии регулятивный карт-бланш, закон пытается уравновесить его введением координационного совета по контролю за ходом эксперимента, но не описывает ни его состав, ни полномочия. Положение о совете утверждено в декабре 2020 года (секретарем Совета по должности будет один из заместителей мэра), однако сам совет до сих пор не сформирован.

Что дальше?

Сфера применения технологии распознавания лиц постоянно расширяется: теперь она используется в системах управления доступом и организации пропускного режима на предприятиях; в сфере торговли и услуг для оплаты «по лицу», профилирования

клиентов, оптимизации обслуживания, борьбы с кражами; помогает организовать учет рабочего времени; создает новые цифровые развлечения; контролирует медицинское освидетельствование и предрейсовые медицинские осмотры в транспортных предприятиях и т.п.

Системы видеонаблюдения не только распознают лица, но и фиксируют пол, возраст, эмоции. В сочетании с развитием искусственного интеллекта и постоянным наполнением различных баз данных это создает условия для качественно нового уровня дискриминации и злоупотреблений — подобно тому, что применяют китайские власти против уйгуров в провинции Синьцзян.

Однако существуют и менее экзотические риски, которые связаны с утечками информации и неавторизованным доступом к системам видеонаблюдения. Более того — само наличие разветвленной сети камер и хранение массива видеозаписей создает угрозу приватности, поскольку ничто не мешает полученные таким образом данные самостоятельно прогнать через программы распознавания лиц, которые становятся все доступнее.

Минимальной гарантией против злоупотребления системами распознавания лиц могло бы стать детальное законодательное описание технологии и пределов ее легального использования, в том числе:

— обязательное подробное и доступное информирования граждан о применении видеонаблюдения и распознавания лиц;

— перечень разрешенных мест использования и гарантированных «чистых» зон, где видеонаблюдение и FR запрещены;

— установление предельного срока хранения с обязательным последующим уничтожением собранных данных;

— обязательный независимый аудит;

— создание эффективных процедур рассмотрения жалоб на нарушения;

— запрет предоставления данных иностранным субъектам, в том числе органам власти.

До законодательного описания технология не должна применяться без ясно выраженного предварительного согласия субъекта.

Вероятнее всего, стандарты приватности, принятые в демократических странах, остановят распространение технологии на определенном этапе, запретят вовсе либо детализируют и регламентируют ее. Там, где под давлением гражданского общества — прежде всего, правозащитных и экспертных организаций — политики пролоббируют законодательные ограничения, применение технологии может оказаться полностью вне закона. В других странах с независимой судебной системой в результате рассмотрения индивидуальных дел возможен запрет применения функции распознавания в общественных местах.

В некоторых юрисдикциях, где высшие суды традиционно стоят на страже конституционных прав и свобод, — ЮАР, Индия — эти запреты могут быть распространены на всю страну вне зависимости от наличия законодательных ограничений.

Жители стран, включенных в региональные механизмы защиты прав человека, доведут дела до международных судов — Суд ЕС, ЕСПЧ, суд ЭКОВАС — и вынудят их выявить баланс между интересами безопасности и частной жизнью, сформировав региональные стандарты. Международные суды неизбежно будут учитывать уже принятые к тому времени решения национальных коллег. Так постепенно сформируется единообразный подход к ограничениям технологии распознавания лиц.

Свободно и бесконтрольно она продолжит применяться лишь в странах, которые, с одной стороны, могут себе позволить закупать и устанавливать в огромных количествах камеры видеонаблюдения и хранилища данных, а с другой — быть достаточно авторитарными и независимыми от международных стандартов, чтобы игнорировать их при попустительстве подконтрольных судов.

В таких странах мы будем наблюдать быстрое и массовое разворачивание стремительно дешевеющей технологии при поддержке лояльных IT-компаний, сопровождающееся убеждением населения в ее необходимости, полезности и

безопасности. А уже затем постфактум законодательное регулирование можно будет адаптировать к сформированной реальности. Подконтрольные властям суды на третьем этапе зафиксируют и одобрят сложившуюся правоприменительную практику.

Противовесов, по сути, никаких нет — ограничить технологический прорыв невозможно. В этих регионах неизбежно возникнут практики противодействия тотальному видеонаблюдению путем скрывания или маскировки лиц либо даже физического уничтожения камер, что мы уже наблюдали в Гонконге.

Дамир ГАЙНУТДИНОВ, к.ю.н., руководитель «Сетевых Свобод»

Кирилл КОРОТЕЕВ, руководитель международной практики Агоры