ARTICLE 19

Под наблюдением:
биометрические технологии и свобода выражения мнений

2021

Впервые опубликовано АРТИКЛЬ 19 в апреле 2021 года

ARTICLE 19
Центр свободы слова
Эл. почта: info@article19.org
Веб-сайт: www.article19.org
Твиттер: @article19org
Фейсбук: facebook.com/article19org

Содержание

Резюме

В данной аналитической записке отражена позиция АРТИКЛЬ 19 о воздействии разработки и применения биометрических технологий на право на свободу выражения мнений.

Подготовка аналитической записки вызвана обеспокоенностью растущим использованием биометрических технологий как частным сектором экономики, так и государственными органами. Биометрические технологии используются для анализа действий, внешности и выражения мнения людьми в общественной и частной жизни. Их использование варьируется от контроля границ до разблокировки смартфонов, и ясно одно: они все чаще воспринимаются как норма повседневной жизни. Эти технологии могут изменить поведение людей в публичных местах и, соответственно, поставить под угрозу само существование гражданского пространства – важнейшей опоры демократии, обеспечивающей открытое участие в обсуждении вопросов, представляющих общественный интерес.

Разработка и использование биометрических технологий должны рассматриваться через призму прав человека, чтобы обеспечить защиту основных прав и свобод. Мы хотели бы обратить особое внимание на следующие вызывающие беспокойство вопросы:

- Возросшая массовая слежка за общественным пространством с использованием биометрических технологий, таких как распознавание лиц и распознавание эмоций, несомненно окажет значительное негативное влияние на свободу выражения мнений и гражданское участие.
- Многие биометрические технологии разрабатываются и применяются в отсутствие адекватной законодательной базы или правовых оснований. Это вызывает серьезную обеспокоенность, поскольку данные технологии, в силу своих особенностей, активно вмешиваются в различные аспекты жизни и оказывают разностороннее влияние на права человека, особенно на гарантии конфиденциальности и защиты данных, а также свободы выражения мнений.
- Наблюдается острый недостаток подотчетности Государственные и частные структуры не предусмотрели эффективных средств правовой защиты потенциальных жертв применения таких технологий. Неясно, каким образом может быть разрешена проблема, например, в случае дискриминации в результате распознавания лиц..
- Наконец, доступность определенной биометрической технологии не должна автоматически оправдывать ее использование. Технологии имеют недостатки, бреши в системах безопасности и базируются на ряде систематических предубеждений. Вместо использования

> технологий для служения человеку или разработки решений существующих проблем, погоня за созданием новый технологий и продуктов исключительно ради самого такого создания является фундаментально ошибочным подходом.

В силу этих причин АРТИКЛЬ 19 предупреждает против использования данных технологий, особенно в целях национальной безопасности или борьбы с терроризмом, без достаточной законодательной базы, гарантирующей защиту прав человека. Мы считаем, что необходим подход, основанный на правах человека, и призываем к мораторию на разработку и использование таких технологий как государственными, так и частными структурами до тех пор, пока они не смогут обеспечить всестороннюю защиту свободы выражения мнений и исполнение международных норм в области прав человека.

Данный документ состоит из пяти частей. Вначале мы представляем историю биометрических технологий и связанную с ними терминологию. Затем кратко перечисляем применимые международные нормы в области обеспечения свободы выражения мнений. Далее следует раздел о нарушениях прав человека, вызванных разработкой и использованием таких технологий, акцентирующий внимание на проблемах, связанных с обеспечением свободы выражения мнений и информации. Затем мы представляем два примера, первый – о воздействии распознавания лиц на свободу выражения мнений и второй – о воздействии распознавания эмоций на реализацию данной свободы. Наконец, мы представляем всесторонние рекомендации для государств, частных компаний и других заинтересованных лиц.

Краткое изложение рекомендаций:

1. массовая слежка с использование биометрических данных должна быть запрещена;
2. необходимо запретить проектирование, разработку и использование технологий распознавания эмоций;
3. необходимо соблюдать принципы правомерности, соразмерности и необходимости при проектировании, разработке и использовании биометрических технологий;
4. государства должны ввести соответствующее законодательное регулирование проектирования, разработки и использования биометрических технологий;
5. проектирование, разработка и использование биометрических технологий должны быть прозрачными и открытыми для общественного обсуждения;

6. необходимо ввести и обеспечить выполнение требований прозрачности работы данного технологического сектора;
7. необходимо гарантировать подотчетность и доступ к средствам правовой защиты в случае нарушения прав человека в результате использования биометрических технологий;
8. частный сектор экономики должен проектировать, разрабатывать и применять биометрические системы в соответствии с нормами в области прав человека.

Введение

По всему миру системы идентификации и верификации полагаются на биометрические данные, от отпечатков пальцев и образцов ДНК до более современных биометрических технологий, с целью идентификации людей на основе их физических черт или поведения.[1] Государственные и частные структуры используют такие технологии в различных контекстах, чтобы в реальном времени измерять и анализировать то, как люди выглядят, говорят, двигаются и ведут себя. Данные технологии используются в таких сферах как борьба с преступностью и пограничный контроль, реклама или маркетинг;[2] они стали популярным способом разблокировки смартфонов, входа в онлайн-банки или доступа в физические или интернет-пространства.[3] Их массовое использование, однако, не обязательно ограничивается идентификацией. Они также применяются для профилирования и категоризации людей на основании возраста, гендера, цвета кожи, их действий и контактов, самочувствия и даже вероятного поведения в будущем.

Быстрое развитие биометрических технологий в последние годы обусловлено двумя основными факторам. Первый – доступность **беспрецедентного числа больших наборов данных**, собранных, прежде всего, частными структурами в рамках моделей ведения бизнеса, все более полагающихся на большие данные, и при поддержке вызывающего опасения нарратива о борьбе с терроризмом и обеспечении общественной безопасности. Второй фактор – растущая доступность и снижающаяся стоимость **машинного обучения**, как с точки зрения оборудования (вычислительные мощности и компьютерные инфраструктуры) и программного обеспечения (включая библиотеки, рост финансирования и вовлечения человеческих ресурсов). Эти два фактора тесно взаимосвязаны, поскольку второму фактору для функционирования необходим первый. Эти достижения способствовали широкому распространению систем наблюдения и перехода от практики использования слежки и идентификации в исключительных случаях, к реальности, в которой они стали нормой.

Хотя технология развивается и становится все более популярной, соответствующая законодательная база не формируется с необходимой скоростью. Хотя многие страны приняли специальные механизмы регулирования биометрических технологий «первого поколения», этого нельзя сказать о новейших технологиях, большая часть которых внедряется в отсутствие специализированной правовой основы. Это крайне проблематично, поскольку биометрические технологии оказывают отрицательное влияние на осуществление прав человека по нескольким направлениям и особым образом вмешиваются в реализацию прав на неприкосновенность частной жизни и защиту данных,[4] уважение достоинства личности,[5] недопущение дискриминации,[6] самоопределение и доступ к эффективным средствам правовой защиты.

Постоянно растущее, повсеместное и зачастую невидимое использование биометрических технологий органами государственной власти и частными структурами вместе с их способностью идентифицировать и отслеживать людей и их поведение также влияет на право на свободу выражения мнений, особенно на возможность сохранять анонимность. Это также драматическим образом влияет на гражданское пространство, где люди осуществляют свои права, участвуют в общественной жизни и собраниях, выражают мнения и получают информацию. Гражданское пространство – основополагающий элемент демократии, повсеместное развертывание и использование биометрических технологий ставит под угрозу само его существование.[7] Также отмечается серьезный недостаток прозрачности того, кто, как и почему разрабатывает и применяет эти технологии. Это препятствует общественному обсуждению их использования государственным органами и частным сектором.

Пандемия COVID-19 привела к активизации призывов положиться на технические решения и придала дополнительный импульс развитию и применению биометрических технологий в качестве «ключевых» инструментов для реализации мер, направленных на борьбу с пандемией, государственными и частными структурами.[8] В их число входят различные приложения для мониторинга соблюдения карантина или отслеживания контактов в целях эпидемиологического расследования,[9] а также использование полицейскими силами шлемов, позволяющих сканировать людей, проходящих мимо них в общественном пространстве, для измерения температуры – симптома типичного для COVID-19.[10] Вызывает тревогу, что и государственные и частные структуры пропагандируют нарратив, противопоставляющий права человека обеспечению общественного здравоохранения,[11] а также подталкивают население принять беспрецедентный уровень массовой слежки. Хотя меры защиты населения от COVID-19 крайне важны и могут быть упрощены при использовании биометрических технологий, технологические решения вряд ли являются панацеей, вопреки обратным утверждениям. В любом случае из-за воздействия данных технологий на осуществление основных прав их использование всегда должно подлежать контролю и соответствовать международным нормам. Нельзя допускать нормализации использования этих технологий в повседневной жизни.

АРТИКЛЬ 19 считает необходимым внести свой вклад в обсуждение принципиальной возможности смягчить воздействие биометрии на свободу выражения мнений и на права человека в целом, либо необходимости введения запрета на использование данных технологий. В данной аналитической записке мы рассматриваем воздействие биометрических технологий на свободу выражения мнений и информации и предлагаем рекомендации для обеспечения свободы выражения мнений государственными органами, частными структурами и другими заинтересованными лицами в контексте использования таких технологий.

Данный документ состоит из следующих частей:

- во-первых, приведены определения основных понятий, используемых в контексте биометрических технологий;
- во-вторых, кратко представлены международные нормы в области прав человека применимые к биометрическим технологиям;
- в-третьих, проведена оценка воздействия биометрических технологий на свободу выражения мнений;
- в-четвертых, рассмотрены два конкретных примера о взаимодействии биометрии и свободы выражения мнений: один связан с распознаванием лиц, второй – с распознаванием эмоций;
- наконец, предложены рекомендации для государственных органов, частных структур и других заинтересованных лиц о том, каким образом необходимо гарантировать защиту свободы выражения мнений при проектировании, разработке и использовании биометрических технологий.

Наши рекомендации для государственных органов, частных компаний и других заинтересованных сторон сопровождаются горячим призывом не изымать из общественного обсуждения один из самых важных вопросов, связанных с правом на свободу выражения мнений и свободу собраний, а также самим существованием гражданского пространства для нашего и последующих поколений.

История развития биометрических технологий

Основные термины

Термин «**биометрия**», как правило, описывает физиологические и поведенческие характеристики людей. В их число могут входить среди прочего отпечатки пальцев, голос, изображение лица, узор сетчатки и радужной оболочки глаза, геометрия ладони, походка или ДНК-профиль.

Биометрические данные получили следующее определение: «личные данные, полученные в результате специализированной технической обработки и связанные с физическими, физиологическими или поведенческими чертами физического лица, позволяющие или подтверждающие однозначную идентификацию этого физического лица, например, изображение лица или дактилоскопические данные (отпечатки пальцев)».[12] Биометрические данные необратимо изменяют связь между телом и идентичностью, поскольку делают характеристики человеческого тела «машиночитаемыми» и открытыми для использования в будущем.[13]

Термин **биометрическая технология**, в свою очередь, обозначает ряд технологий, измеряющих и анализирующих такие уникальные черты человека как ДНК, отпечатки пальцев, голосовой отпечаток, геометрия рук, сетчатка или радужная оболочка глаз, характеристики сердцебиения.[14]

За недавнее время биометрические технологии включили в себя, среди прочего, многофакторную биометрию, поведенческую биометрию, динамическое распознавание лиц, удаленное распознавание по радужной оболочке глаза, а также ряд других применений, находящихся на различных этапах разработки.[15]

Распознавание лиц входит в категорию биометрических технологий и может быть определено как «автоматическая обработка цифровых изображений лиц для контроля, идентификации или категоризации субъектов данных».[16]

Распознавание эмоций – биометрическая технология, использующая машинное обучение в попытке идентифицировать эмоциональные состояния людей и рассортировать их в отдельные категории, такие как злость, удивление, страх, радость и т.д. Исходные данные могут включать в себя изображения лица, движения тела, тон голоса, произнесенные или напечатанные слова и физиологические признаки (например, пульс, кровяное давление, скорость дыхания, жестикуляция и мимика или голос).[17]

Надежность биометрических технологий

Точность и надежность применения биометрических технологий для распознавания эмоций и поведения на настоящий момент не доказаны. Авторы большого числа научных исследований предупреждают, что выражение лица и другое наблюдаемое поведение не являются надежными индикаторами внутреннего эмоционального состояния.[18] Исследователи предупреждают о значительном риске дискриминации расовых, этнических или других меньшинств, а также о расистских предубеждениях, лежащих в основе таких технологий.[19] Даже высокоточные системы не позволили бы избежать этих проблем и имеющихся правовых осложнений. Даже когда биометрические технологии являются эффективными и точными, они уникальным образом вмешиваются в частную жизнь и препятствуют реализации прав человека.

Более того, необходимо отметить, что многие действующие биометрические технологии полагаются на исторические представления, введенные в обиход исследованием фенотипов, вдохновленным расовой классификацией и расистскими предубеждениями (лицевой угол, краниоскопия/френология, физиогномика, антропометрия).[20] Такие технологии были созданы для обоснования так называемого «научного» расизма в колониальном мире.[21] Хотя научная обоснованность этих методов никогда не была подтверждена, применение таких техник отразилось на образе мышления, повлиявшего на развитие данной технологии, прежде всего для профилирования, классификации и идентификации в целях уголовной антропологии и определения евгенических параметров.[22] Таким образом, социальная история биометрических технологий критически важна для понимания проблем, связанных с их сегодняшним использованием.

Это означает, что допустимость внедрения биометрии должна быть жестко связана с уравновешиванием законного интереса к использованию таких технологий, с одной стороны, а с другой – необходимости гарантировать обеспечение прав человека.

Основные способы применения и нарративы об использовании биометрических технологий

Биометрические технологии в настоящее время используются различными способами и в различных целях. Наиболее значимые перечислены ниже.

- Защита **национальной безопасности, контртеррористические меры, предупреждение и борьба с преступностью** широко используются для обоснования применения биометрических технологий в различных контекстах в течение последних двух десятилетий, начиная с контроля и управления потоками на границах[23] до национальных систем идентификации.[24] Помимо нарративов об порядке и безопасности,

правоохранительные органы используют технологии распознавания лиц как инструмент, который потенциально может способствовать предотвращению и раскрытию преступлений, обеспечивать общественную безопасность и привлекать к ответственности виновных,[25] а также для предотвращения мошенничества и краж, либо для отслеживания перемещений меньшинств.[26]

- Биометрические технологии использовались органами государственной власти для управления доступом на различные государственные мероприятия и для **оказания государственных услуг**,[27] среди примеров электронные системы здравоохранения и ведение списков избирателей.[28] К ним также обращаются пользователи из частного сектора экономики или межсекторальные инициативы под руководством частных структур, например, при **разработке проектов «умных городов»**, систем общественного транспорта, доступа в школы, другие физические или онлайн-пространства.[29]

Использование биометрических технологий обычно обосновывается перечислением ряда преимуществ, которые они, как предполагается, обеспечивают. Среди них быстрый и беспрепятственный доступ, экономичные решения, точность и надежность, более высокая степень безопасности, улучшение социального обеспечения. Однако большая часть этих преимуществ либо не подтверждаются, либо их оценка не учитывает серьезные компромиссы в сфере обеспечения прав человека.

Более того, мы стали свидетелями широкого использования заявлений о том, что сама по себе доступность технологий достаточна для обоснования их использования. Мы должны решительно выступить против такого подхода. Биометрические технологии не нейтральны. На техническом уровне биометрия полагается на большое число допущений; на институциональном уровне технологии используются в корне дискриминационными способами, усугубляющими неблагоприятное социальное положение и исторически сложившуюся дискриминацию. В более общем смысле, биометрические технологии действуют как социотехнические системы, отражающие ценности и предубеждения, которые, как демонстрирует данная аналитическая записка, не учитывают правозащитные нормы, а, возможно, и несовместимы с ними.[30]

Международные стандарты в области прав человека и биометрические технологии

Применимые правозащитные стандарты

Не существует международных стандартов, напрямую регулирующих биометрические технологии, однако их внедрение и использование затрагивают ряд прав человека, в частности:

- **Право на свободу выражения мнений** гарантированно Статьей 19 Всеобщей декларации прав человека[31] и наделено юридической силой Статьей 19 Международного пакта о гражданских и политических правах (МПГПП),[32] а также региональными договорами о правах человека.[33] В соответствии с международными стандартами в области прав человека, ограничения права на свободу выражения мнений допускаются только в ряде особых обстоятельств (так называемый «трехчастный тест»); все ограничения должны быть четко сформулированы и не могут подрывать реализацию данного права.[34]
- **Право на доступ к информации** признано в качестве составляющей права на свободу выражения мнений. Комитет ООН по правам человека как орган уполномоченный интерпретировать положения МПГПП интерпретировал объем и ограничения права на доступ к информации в 2011 г., заявив, что Статья 19 МПГПП обеспечивает право на доступ к информации, находящейся в распоряжении органов государственной власти. Она также предусматривает активное распространение государствами информации, имеющей общественное значение, и обеспечение к ней «легкого, эффективного и практического» доступа.[35] Комитет также указал, что государства должны принять «необходимые процедуры», например, законодательство, для эффективного осуществления права на доступ к информации, чтобы плата за доступ к информации была ограниченной, а запросы обрабатывались своевременно. Также органам власти необходимо предоставлять объяснение в случае отказа в информации, помимо этого государства должны предусмотреть механизмы обжалования отказов в предоставлении информации.[36]
- **Право на мирные собрания** гарантировано первым параграфом Статьи 20 Всеобщей декларации прав человека и наделено юридической силой Статьей 21 МПГПП, Статьей 5(d) Конвенции о ликвидации расовой дискриминации[37] и региональными договорами.[38] Данные нормы требуют, чтобы допустимые ограничения права проходили трехчастный тест, как и ограничения права на свободу выражения мнений.[39]
- **Право на неприкосновенность частной жизни** гарантировано Статьей 12 Всеобщей декларация прав человека и Статьей 17 МПГПП, а также

региональными договорами.[40] В соответствии с данными нормами, частная жизнь является широким понятием, связанным с защитой личной независимости и взаимоотношений между отдельным человеком и обществом, включая правительства, компании и других людей. Право на неприкосновенность частной жизни признано в качестве основного права, на котором основывается обеспечение человеческого достоинства и других ценностей. Ограничения неприкосновенности частной жизни также должны проходить трехчастный тест.[41]

- **Право на недискриминацию и право на равенство** защищены Статьей 2 и Статьей 7 Всеобщей декларации прав человека и наделены юридической силой Статьями 2 и 26 МПГПП, Статьей 2(2) Международного пакта об экономических, социальных и культурных правах, а также региональными договорами и инструментами.[42] Право на равенство предполагает, что всем людям должна быть гарантирована «равная и эффективная защита против дискриминации по какому бы то ни было признаку, как-то расы, цвета кожи, пола, языка, религии, политических или иных убеждений, национального или социального происхождения, имущественного положения, рождения или иного обстоятельства».[43]

Свобода выражения мнений и неприкосновенность частной жизни являются взаимоукрепляющими, особенно в цифровом веке.[44] Неприкосновенность частной жизни является необходимым условием для существования свободы выражения мнений: без нее у людей нет пространства для размышлений, высказываний и формирования собственного мнения. Из этого следует, по мере вмешательства разработки и внедрения государствами биометрических технологий в реализацию права на неприкосновенность частной жизни, каждый новый способ их применения необходимо подвергать проверке с использованием трехчастного теста на законность, соразмерность и необходимость.

Кроме того, **защита персональных данных** (защита данных) признана Комитетом по правам человека ООН (КПЧ ООН), в чьи обязанности входит интерпретация МПГПП, основополагающей частью неприкосновенности частной жизни.[45] Резолюция Генеральной Ассамблеи ООН от 1990 г. относительно руководящих принципов регламентации компьютеризированных картотек, содержащих данные личного характера,[46] излагает шесть основных принципов защиты данных, основанных на справедливом использовании информации. На региональном уровне защита персональных данных также гарантирована Конвенцией Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (Конвенция №108),[47] Хартией ЕС,[48] Конвенцией по кибербезопасности и защите персональных данных Африканского союза (Конвенция АС о киберпреступности)[49] и Принципами защиты неприкосновенности частной жизни и персональных данных Организации американских государств.[50]

Международное право в области прав человека также признает, что если человек хочет узнать, является ли он субъектом применения биометрических технологий органами государственной власти, и если да – по какой причине, то он или она имеют право получить информацию в соответствии с законодательством о защите данных. Среди этих прав – право на информирование о сборе и использовании персональных данных, что ведет к ряду обязательств, связанных с предоставлением информации контроллером.[51] Данное право получило широкое признание в международном праве, а также вошло в основные региональные соглашения о защите данных. Комитет ООН по правам человека в Замечании общего порядка № 16 отметил, что данное право необходимо для обеспечения права на неприкосновенность частной жизни.[52] Данное право получило широкое применение в инструментах международного права, а также в важнейших региональных соглашениях о защите данных.[53] Общим регламентом ЕС по защите данных[54] каждый человек наделен правом получать информацию. Регламент проводит различие между двумя сценариями: с одной стороны, если персональные данные были получены напрямую от субъекта данных (Статья 13), с другой стороны – если данные были получены не от субъекта данных (Статья 14).

Важность обеспечения гарантий против неправомерного доступа к данным итребований прозрачности была подчеркнута в Европейском Союзе Агентством по основным правам с особым акцентом на сбор персональных данных, включая отпечатки пальцев, соискателей статуса беженца и лиц, обращающихся за визами, а также мигрантов с неурегулированным статусом.[55] Некоторые государства также включили в национальное законодательство защиту этих прав и гарантии сохранения неприкосновенности частной жизни.[56]

Международные правозащитные органы также начали приходить к признанию **права на анонимность** в качестве важного аспекта права на свободу выражения мнений и неприкосновенность частной жизни. Это отражается на использовании биометрических технологий для идентификации людей в их домах и в общественных местах. Соответственно, воспрепятствование государством сохранению анонимности должно проходить трехчастный тест на законность, соразмерность и необходимость, как и любое другое вмешательство в реализацию данных прав.[57]

Стандарты в области прав человека и биометрические технологии

Хотя отсутствуют международные стандарты, особым образом регулирующие биометрические технологии, в настоящее время формируется свод норм, затрагивающих их разработку и внедрение.

Прежде всего, правозащитные органы все более широко признают воздействие новых форм обработки данных на права человека. Например, в отношении профилирования, которое может включать в себя использование биометрических систем для получения, анализа и прогнозирования информации о людях с целью оценки каких-либо их характеристик, Совет по правам человека ООН с обеспокоенностью отметил в марте 2017 г., что:

> Автоматизированная обработка персональных данных в целях индивидуального профилирования может приводить к дискриминации или принятию решений, которые могут иным образом негативно повлиять на осуществление прав человека, включая экономические, социальные и культурные права.[58]

Во-вторых, напрямую связаны с биометрическими данными:

- Модернизированная Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (Конвенция №108+) разрешает использование биометрических данных, однозначно идентифицирующих человека, исключительно при условии, что соответствующие гарантии закреплены законодательно, дополняя Конвенцию №108.[59]
- Общий регламент ЕС по защите данных запрещает обработку биометрических данных с целью однозначной идентификации физических лиц за некоторыми исключениями.[60] Кроме того, Общий регламент ЕС по защите данных рассматривает биометрические данные, используемые с целью идентификации, как «данные особой категории», то есть они считаются более конфиденциальными и нуждаются в дополнительной защите. Сходный подход принят Стандартами защиты персональных данных Иберо-американских государств.[61]
- Конвенция АС о киберпреступности вводит требование о получении предварительного разрешения на обработку персональных данных, включающих в себя биометрические данные, у национального органа по защите данных.[62]

Другие международные документы содержат полезные указания для оценки использования биометрических технологий и их воздействия на права человека. Например, Верховный комиссар ООН по правам человека в своем докладе о праве на неприкосновенность частной жизни в цифровой век подчеркнул обеспокоенность использованием биометрических данных и возможностью для «вопиющих злоупотреблений», а также осуществление государствами проектов, полагающихся на биометрию, в отсутствие «адекватных правовых и процессуальных гарантий».[63] В Докладе государствам рекомендовано среди прочего:

> Обеспечить, чтобы системы, использующие большие объемы данных, включая системы, предусматривающие сбор и хранение биометрических данных, внедрялись только тогда, когда государства могут доказать, что они являются необходимыми и соразмерными для достижения законной цели.[64]

Более того, три специальных докладчика по правам человека уже предупредили о рисках биометрических систем:

- В 2019 г. Специальный докладчик ООН по вопросу о праве на свободу мирных собраний и на свободу ассоциаций заявил в своем докладе, что «использование шпионских методов для неизбирательной массовой слежки за теми, кто осуществляет свое право на мирные собрания и ассоциации, как в реальном, так и в цифровом пространстве, должно быть запрещено».[65]
- Специальный докладчик ООН по вопросу о праве на неприкосновенность частной жизни поставил под сомнение необходимость и пропорциональность биометрических систем.[66]
- Специальный докладчик ООН по вопросу о праве на свободу убеждений и их свободное выражение озвучил сходную обеспокоенность воздействием биометрических систем на правозащитников, журналистов, политиков и следователей ООН.[67]

В прецедентном праве международных органов, региональных и национальных судов также предусмотрены общие указания относительно стандартов, применимых в ходе использования биометрических технологий. В частности, Европейский суд по правам человека (ЕСПЧ) подчеркнул необходимость обеспечить баланс между защитой основных прав и разработкой новых технологий и постановил, что «повсеместное и тотальное» хранение биометрических данных является «чрезмерным вмешательством» в реализацию права на неприкосновенность частной жизни, поскольку это не соответствует требованиям ЕСПЧ и не может считаться «необходимым в демократическом обществе».[68]

Несколько отличный подход, очевидно, используется в целях **борьбы с терроризмом**. В 2017 г. Совет Безопасности ООН принял решение о разработке и введении в действие системы сбора и обмена биометрическими данными в целях борьбы с терроризмом на уровне государств.[69] Сходным образом в Дополнении к Мадридским Руководящим принципам 2018 г. отмечена полезность биометрических данных.[70] В результате биометрические системы считаются легитимным инструментом для идентификации подозреваемых в террористической деятельности.

Тем не менее, даже в целях борьбы с терроризмом использование биометрических технологий должно соответствовать международным

стандартам, в частности, принципам необходимости и соразмерности. Сборник практических рекомендаций ООН по ответственному использованию биометрических данных и обмену ими в рамках борьбы с терроризмом[71] может рассматриваться в качестве первого шага к введению подхода ориентированного на права человека, но на настоящий момент в нем не представлена адекватная основа для решения данной проблемы.

Обязанности частного сектора по обеспечению прав человека

При том, что международное право в области прав человека налагает на государства обязательства защищать и соблюдать права человека, широко признано, что частный сектор также несет ответственность за соблюдение прав человека.[72]

Руководящие принципы предпринимательской деятельности в аспекте прав человека (Руководящие принципы) представляют собой отправную точку для оформления роли частного сектора в защите прав человека в интернете.[73] В них признана ответственность коммерческих компаний соблюдать права человека вне зависимости от правозащитных обязательств, взятых на себя государствами, и рекомендован ряд мер, которые необходимо принять компаниям.[74] В их число входят включение гарантий прав человека уже на стадии проектирования с целью смягчения их неблагоприятного воздействия, усиление координации для оказания коллективного влияния на государственные органы, а также предоставление средств правовой защиты в случае возникновения неблагоприятных последствий для реализации прав человека.

Различные заинтересованные стороны призывают к введению регулирования биометрических технологий. В ограниченной степени, в их число входят и высокотехнологичные компании, которые, среагировав на ранние призывы ввести стандарты для «этических» или «надежных» биометрических технологий, начали признавать необходимость дополнительных шагов, а также начали выступать за введение регулирования. Однако недостаточно ни «этических», ни регулятивных мер, предложенных компаниями технологического сектора. Они чаще всего представляют собой призывы к мягким мерам, а не предложения об учреждении нормативной базы для защиты прав человека при применении биометрии.[75]

Наконец, растет признание того, что права человека должны лежать в основе **технических стандартов** и **протоколов**, поскольку протоколы могут оказывать значительное воздействие на применение стандартов.[76] Однако, несмотря на это, права человека не упоминаются напрямую в соответствующих процедурных

документах значительной части технологических и коммерческих компаний, хотя эти структуры быстро становятся шлюзами и посредниками при реализации свободы выражения мнений и свободы мирных собраний, поскольку они разрабатывают большую часть систем, использующих биометрические технологии. Такие инициативы, как Принципы Искусственного интеллекта компании Google,[77] могут рассматриваться как шаг в этом направлении, однако, они продемонстрировали свои ограничения и до настоящего времени они не смогли обеспечить необходимый уровень прозрачности и подотчетности для этих компаний.

Биометрические технологии и право на свободу выражения мнений и информации

Биометрические технологии и права человека: общие проблемы

До обсуждения последствий применения биометрических технологий непосредственно на реализацию права на свободу выражения мнений иинформацию АРТИКЛЬ 19 хотела бы подчеркнуть общие правозащитные проблемы, связанные с данными технологиями.

Сбор и хранение данных

Разработка и внедрение биометрических технологий подразумевает сбор и обработку большого объема конфиденциальных персональных данных. Биометрические данные представляют собой особую категорию персональных данных, требующих дополнительных гарантий защиты в силу того, что они способны раскрыть личную информацию (расовое или этническое происхождение, пол и т.д.). По своей природе биометрические технологии значительным образом вмешиваются в реализацию прав и свобод. Более того, базы данных часто создаются с использованием неоднозначных методов сбора информации (например, выборки данных могут быть нерепрезентативными и не включать в себя все группы населения в равной мере) и содержат предвзятые допущения, отражающие существующие модели социальных стереотипов.[78]

В равной мере проблематична распространенная практика неизбирательного хранения биометрических данных, непрошедшая тест на необходимость и соразмерность.[79] Другими словами, операторы часто хранят биометрические данные дольше, чем это необходимо в первоначальных целях сбора данных.

Более того, большие массивы данных могут быть перепрофилированы, соответственно, возникает проблема расширения сферы применения или охвата технологий для сбора данных и/или выполнения функций, не включенных в полученное разрешение на обработку данных. Уже существуют свидетельства злоупотребления биометрическими базами данных или их использования в первоначально не заявленных целях.[80] В таких случаях даже при получении разрешения субъектов данных на использование их биометрических данных для определенной цели, такое разрешение не включает в себя возможность перепрофилирования базы данных, что должно считаться незаконным.

Возможные нарушения безопасности

Нарушения безопасности баз данных трудно обнаружить и дорого устранить. Еще сложнее отдельным субъектам данных добиться возмещения ущерба, если им причинен вред в результате таких нарушений безопасности. Действительно, биометрические данные – это не пароли, которые можно изменить, в случае их утечки. Напротив, они могут использоваться для идентификации и отслеживания человека в течение всей жизни. Угрозы безопасности еще выше в случае крупномасштабных и централизованных баз данных и несут особый вред для маргинализированных сообществ, поэтому, возможность создания централизованных баз может рассматриваться только в случае крайней необходимости и в отсутствие альтернатив.[81]

Наконец, угрозы безопасности выше в странах, где высокотехнологичная индустрия и инфраструктура безопасности данных не существуют или недостаточно развиты. При отсутствии доверия вызывает глубокую обеспокоенность централизованное хранение правительственными органами или другими структурами биометрических данных граждан.

Проблема «черного ящика»

Новые способы применения биометрических технологий все более полагаются на машинное обучение, что ставит вопрос о проблеме «черного ящика».[82] Непроницаемость процессов и систем машинного обучения представляет собой фундаментальную проблему для обеспечения подотчетности и оказания правовой помощи в контексте автоматизированного принятия решений. С учетом большой вероятности когнитивных искажений в пользу автоматизированных решений, что усугубляется несовершенными и громоздкими техническими системами, сложно или невозможно оспорить результаты автоматизированного профилирования или подбора соответствий, особенно, когда неясны логика и предпосылки, используемые системами для принятия решений. Как следствие, судам сложно или невозможно судить о достоверности доказательных заявлений.

Масштаб

Биометрические технологии в настоящее время внедряются в беспрецедентных масштабах, что может привести к массовой слежке в различных регионах мира. От аэропортов до площадей, от инфракрасных камер до систем идентификации по венам ладони – использование технологий для идентификации и слежки становится все более распространенным.[83]

Неадекватные национальные законодательные базы

Неадекватная или отсутствующая правовая база для разработки и внедрения биометрических технологий представляет собой серьезную проблему.

Законодательство о защите данных (если оно существует) хотя и является необходимым, может быть недостаточным для разрешения всех проблем. Адекватная законодательная база должна среди прочего содержать четкие нормы о согласии, законной обработке, ограничении целей сбора данных. Кроме того, ряд механизмов защиты данных предусматривает исключения для использования персональных данных в правоохранительных целях. Такие исключения часто сформулированы широко и не предусматривают необходимых гарантий защиты персональных данных. Для разработки и использования биометрических технологий как государственными, так и частными структурами необходима надлежащая законодательная база, соответствующая международным стандартам.

Необходимость и соразмерность

Биометрические технологии разрабатываются и внедряются для достижения постоянно растущего числа целей. Наличие технологии часто считается достаточной причиной для ее применения без адекватной оценки законности целей ее использования. Нельзя допускать разработку и внедрение таких технологий в целях, которые подрывают человеческое достоинство, например, для тотальной цифровой слежки, унижения или манипуляции.[84] Даже если установлена законная цель для использования биометрии, использование таких технологий не всегда проходит четко сформулированный тест на необходимость и соразмерность: технология должна быть абсолютно необходимой для заявленной цели и также должны отсутствовать средства для ее достижения, в меньшей мере препятствующие реализации основных прав и свобод. Если данный тест не пройден, технология не должна использоваться вне зависимости от ее доступности или привлекательности.[85]

Отсутствие средств правовой защиты в случае нарушений прав человека

Ни государственные, ни частные структуры, использующие биометрические технологии, не предусмотрели эффективные средства правовой защиты в случае нарушения прав человека. Например, если использование биометрических технологий ведет к дискриминации, неясно, каким образом данная ситуация может быть разрешена. Сходным образом при использовании полицией биометрических технологий для мониторинга людей, выражающих политические, религиозные или другие защищенные мнения, неясно, какие средства правовой защиты доступны этим людям. В любом случае необходимым условием для реализации права на эффективные средства правовой защиты является знание людей о том, что их биометрические данные обрабатываются, или что затрагивающее их решение принимается на базе биометрических технологий. В подавляющем большинстве случаев – это не так.

Биометрические технологии и препятствия для свободы выражения мнений и права на информацию

Часть последствий использования биометрических технологий для реализации права на свободу выражения мнений и информации принципиальным образом не отличается от вызовов, созданных более ранними технологиями, а остальные вызваны специфическими характеристиками биометрии. В их число входят:

Негативное воздействие массовой слежки на реализацию свободы выражения мнений

Хотя право в области прав человека развивается и включает в себя понимание, что защита от незаконной или произвольной массовой слежки, прежде всего, гарантирована правом на неприкосновенность частной жизни,[86] ширится признание того, что массовая слежка также оказывает негативное воздействие на свободу выражения мнений.[87] Если биометрические технологии используются для идентификации и профилирования в общественных местах, например, технологии распознавания лиц для обработки изображений лиц, зафиксированных видеокамерами на улицах, площадях, в метро, на стадионах или в концертных залах, то они лишают людей возможности безопасно общаться, сохраняя анонимность, а также анонимно перемещаться и находиться в общественных местах. Использование данных технологий напрямую вредит работе неправительственных организаций, поскольку препятствует защите их источников, а также осуществлению ими контрольной функции.[88] Исследования демонстрируют, что осознание людьми того, что за ними наблюдают, может привести к отказу от участия в публичных собраниях, в социальной или культурной жизни, от свободного выражения мыслей, мнений и религиозных убеждений в общественном пространстве.[89]

Воздействие на свободу выражения мнений отдельных категорий людей

Использование биометрических технологий может оказывать более серьезное воздействие на право на свободу выражения мнений определенных категорий людей, которые могут стать объектом особого внимания в силу реализации ими этого права, что также может затрагивать представителей меньшинств. Например, может быть ограничена возможность проводить журналистские расследования или устанавливать контакты с источниками информации, если журналисты знают, что за ними могут следить и идентифицировать с использованием биометрических технологий в общественных или частных пространствах.[90] Страх оказаться под наблюдением может оказывать на них сильное сдерживающее воздействие, что, в свою очередь, может негативно сказываться на качестве журналистских материалов и расследований, подрывая роль средств массовой информации в обществе. Активисты и политическая оппозиция могут испытывать аналогичные опасения

и, соответственно, стимулы для самоцензуры. Например, они могут отказаться от реализации своего права на протест, если в случае использования биометрических технологий государством, их могут квалифицировать определенным образом, например, за повторные протесты и т.д.[91]

Необходимость обеспечения прозрачности и доступа к информации

Широко распространенное внедрение биометрических технологий и сбор чрезмерных баз данных совместно с повсеместным отсутствием прозрачности принципов внедрения и использования таких технологий также создают проблемы в связи с реализацией права на доступ к информации. Когда правительства собирают и хранят огромное количество биометрических данных, критически важно право общественности знать, что происходит с этой информацией. В этой связи возникает особая сложность, когда технологии применяются для идентификации и верификации в общественных местах.

Фактически отсутствует информация о том, кто разрабатывает биометрические технологии, какие технологии разрабатываются, а также кто, как и в каких целях их внедряет. Помимо этого, неизвестно, проводят ли разработчики и продавцы комплексную юридическую оценку покупателей технологий на предмет соблюдениями ими прав человека.[92]

Государственные и частные структуры тесно сотрудничают на рынках биометрических технологий. При этом не публикуются содержание и условия государственно-частных партнерств и государственных контрактов по закупке технологий органами государственной власти. В целом государства не раскрывают свои взаимоотношения с разработчиками технологий, включая критерии принятия решений о государственных закупках. Отсутствие прозрачности и секретность ведут к тому, что биометрические технологии продаются и используются без должного общественного контроля, со слабыми процедурными гарантиями и неэффективным надзором. Сходным образом органы государственной власти, работающие с биометрическими технологиями, судя по всему, не проводят адекватную оценку последствий их внедрения, что представляет собой важный элемент обеспечения подотчетности.[93]

Законы, гарантирующие свободу информации и право на доступ к информации, – основополагающий юридический механизм, которым могут воспользоваться частные лица, журналисты и активисты для обеспечения прозрачного функционирования органов власти и использования органами власти биометрических данных.[94] Однако попытки доступа к информации об использовании биометрических технологий, находящейся в распоряжении органов власти в рамках законов, обеспечивающих право на информацию, сталкиваются с большим числом препятствий.[95] При несомненном интересе общественности к системе хранения и обработки значительного объема

биометрических данных,[96] особенно с учетом числа людей, чьи данные хранятся в таких базах, органы власти зачастую не публикуют информацию, например, о системах идентификации. Зачастую такая информация публикуется только в результате судебного решения при оспаривании отказа в публикации информации. Судебные апелляции во многих юрисдикциях являются дорогостоящими и требуют значительного времени, поэтому от них часто отказываются стороны, запрашивающие информацию, в том числе журналисты, ученые и активисты.

Также необходимо отметить, что существует инициативы, учитывающие отсутствие прозрачности использования биометрических технологий, и признавшие, что политика в этой области должна быть согласована с этическими аспектами, а меры регулирования должны быть основаны на открытости и прозрачности.[97]

Биометрические технологии и свобода выражения мнений: анализ примеров из практики

Распознавание лиц

Цели и применение технологий распознавания лиц

Распознавание лиц – автоматическая обработка цифровых изображений, содержащих лица людей, в трех основных целях:

- **верификация**, которая включает в себя сравнение двух шаблонов биометрических данных с целью проверки того, фигурирует ли в них одно и то же лицо (сравнение один к одному);
- **идентификация**, которая подразумевает сравнение шаблона биометрических данных с другими шаблонами в базе данных с целью верификации присутствия субъекта данных в базе (сравнение «один ко многим»). Когда распознавание лиц используется в этих целях, его также называют «распознаванием лиц в автоматизированном режиме или в режиме реального времени». Хотя оба способа, как один к одному, таки и один ко многим, связаны с рядом проблем,[98] использование распознавания лиц «один ко многим» в целях идентификации наибольшим образом воздействует на свободу выражения мнений;
- **категоризация** используется для профилирования людей на основании их личных характеристик, таких как пол, возраст и этническое происхождение.[99]

Внедрение технологии распознавания лиц стабильно растет в последние годы. На государственном и муниципальном уровне по всему миру обсуждается введение правил, предусматривающих массовое использование распознавания лиц в публичных пространствах в правоохранительных целях.[100] В некоторых странах риторика обеспечения общественной безопасности широко используется для оправдания постоянного растущей слежки за общественными пространствами.[101]

В свою очередь, частные структуры используют распознавание лиц в разнообразных целях. Например, тысячи розничных продавцов используют распознавание лиц, чтобы сравнивать посетителей магазинов с изображениями известных магазинных воров.[102] Некоторые идут еще дальше и используют распознавание лиц для отслеживания реакции посетителей на товары,[103] или в качестве системы для осуществления покупок.[104] Организаторы развлекательных мероприятий используют распознавание лиц для идентификации владельцев билетов и обеспечения их доступа к услугам или местам проведения мероприятий. Транспортные компании используют системы

распознавания лиц в рекламных щитах, размещенных на станциях метро, для определения реакции на рекламу (удовольствие, недовольство, удивление и нейтральную реакцию) и ее предполагаемой связи с физиологическими характеристиками (возраст и пол),[105] либо для защиты от мошенничества и идентификации водителей.[106] Как было упомянуто ранее, ряд производителей смартфонов дают возможность пользователям разблокировать телефон с использованием функции распознавания лиц.[107]

С другой стороны, на региональном уровне ряд муниципалитетов движутся в противоположном направлении и запрещают использование распознавание лиц в определенных целях.[108] Сходным образом ряд разработчиков технологий распознавания лиц недавно предприняли (хоть и ограниченные) шаги для ограничения или заморозки их разработки и внедрения.[109] Насколько они готовы соблюдать собственные обещания пока не ясно, но такие шаги могут рассматриваться как признание растущего давления ограничить или запретить неизбирательное применение распознавания лиц в правоохранительных целях. В любом случае очень немногие высказывают свою озабоченность, либо не придают равной значимости опасности внедрения систем распознавания лиц частным сектором по сравнению с государственным. Недостаточный интерес к этой проблеме резко контрастирует со все более широким применением распознавания лиц частным сектором, что включает в себя как узкое и локализированное использование, так и широкомасштабное внедрение технологий.[110]

Пандемия COVID-19 привлекла дополнительное внимание к технологиям распознавания лиц. Разработчики воспользовались этой чрезвычайной ситуацией в области охраны здоровья, чтобы внедрить новые способы использования и расширить применение распознавания лиц государственными и частными структурами, в то время как правительства все чаще используют данную технологию для целей мониторинга, обеспечения соблюдения карантина и эпидемиологического контроля.[111] Активные усилия для распространения технологий распознавания лиц настолько велики, что разработчики уже ищут решение технических проблем, созданных обязательным или рекомендованным использованием масок в качестве меры по борьбе с пандемией. Ряд компаний начали разрабатывать алгоритмы «периокулярного» распознавания, которые находят и распознают лица на основе только части лица между скулами и бровями.[112] При этом технология распознавания лиц предлагается как одно из решений проблем, связанных с COVID-19, в отсутствие каких-либо подтверждений, что такая мера имеет какой-либо положительный эффект или хотя бы работает корректно при использовании масок. Такие инициативы, судя по всему, представляют собой часть широкомасштабных усилий для расширения внедрения систем обеспечения слежки в качестве базового компонента борьбы с пандемией.[113]

Правозащитные проблемы, связанные с технологиями распознавания лиц

Всякое использование технологий распознавания лиц, будь то государственным или частным сектором, оказывает воздействие на реализацию прав человека. В ряде случаев распознавание лиц более опасно при использовании частным сектором. Потребителей часто убеждают использовать эти технологии в частной жизни (дома, в отношениях с семьей, друзьями или на работе) во все более легкомысленных целях, ни одна из которых не оправдывает и не является соразмерной нарушениям прав человека, связанным с использованием распознавания лиц.

Многие проблемы, связанные с внедрением и использованием распознавания лиц, сходны с проблемами, вызванными другими биометрическими технологиями. Эта технология часто внедряется в отсутствие специализированной правовой базы, либо каких-либо адекватных гарантий прав человека и без предварительного общественного обсуждения. Однако в силу своих специфических черт, технологии распознавания лиц могут создавать более серьезные сложности для реализации прав человека и свободы выражения мнений, чем другие биометрические технологии. Это вызвано тем, что распознавание лиц имеет две особенности: с одной стороны, данные могут быть собраны без оповещения их субъекта, с другой стороны, данные могут отражать характеристики, пользующиеся защитой международного права (раса, религия, пол и др.).

Среди основных проблем:

- **Согласие**: технологии распознавания лиц не требуют прямого контакта или активных действий субъектов данных. По этой причине людей легко подвергать распознаванию лиц, без их оповещения и согласия.[114] Например, некоторые социальные сети, в частности Facebook, в числе первых разработчиков технологии распознавания лиц, значительным образом полагались на изображения лиц своих пользователей для тренировки системы распознавания лиц, не информируя их и не запрашивая согласия.[115] Даже когда использование распознавания лиц не является скрытым, может быть сложно установить, было ли дано юридически действительное согласие. Например, исследователи считают, что использование Facebook распознавания лиц в любом случае не соответствует стандартам получения информированного согласия в силу сокрытия рисков и нарушения коллективной автономии.[116]
- **Недостаточная прозрачность**: хотя недостаток прозрачности является общей проблемой биометрических технологий, распознавание лиц представляет собой еще более серьезную сложность в силу высокой степени вмешательства данной технологии в частную жизнь. Как

было указано выше, изображение лица может быть сделано без ведома субъекта данных. Такая практика вместе с недостаточной прозрачностью внедрения технологии государственными и частными структурами ведет к тому, что люди не имеют никакой информации о ее использовании и являются легкой целью для злоупотреблений и ненадлежащего использования технологии.

- **Точность**: как и другие биометрические технологии, распознавание лиц основано на статистической оценке соответствия сравниваемых элементов, соответственно, по своей сути, ненадежно. Значительное число исследователей продемонстрировали, что распознавание лиц является неточным, особенно когда его используют в отношении групп, не имеющих достаточного представительства или исторически находящихся в уязвимом положении.[117] Чтобы освободить распознавание лиц от предубеждений необходимо обеспечить среди прочего качество и полноту баз данных, используемых для тренировки алгоритмов. Если не обеспечено качество данных, либо в базах излишним или недостаточным образом представлены определенные характеристики, то результаты распознавания лиц не являются надежными.[118] Это представляет собой особую проблему в случае расовых предубеждений.[119] Точность распознавания лиц чрезвычайно важна, а ошибочное опознавание – более чем неудобство и может иметь серьезные последствия. Например, ложноотрицательный результат поиска «один к одному» может привести к недопуску человека к услугам или в помещение. Ложноположительный результат поиска «один ко многим» указывает неверное соответствие в списке кандидатов, что требует дальнейшего расследования или присвоению определенной маркировки, в таких случаях исправить ситуацию представляется трудным или невозможным.[120]
- **Слабый или отсутствующий правовой надзор**: за рядом исключений, в различных странах фактически отсутствует правовой надзор за использованием распознавания лиц правоохранительными органами. В большинстве случаев не введен прямой запрет на использование органами власти распознавания лиц с камер наблюдения, что превращает прохожих в неосведомленных участников виртуального полицейского опознания. Отсутствуют нормы, регулирующие хранение данных, собранных в рамках распознавания лиц. Обеспокоенность также связана с использованием данной технологии частными структурами: в отсутствие надлежащего надзора, компании внедряют распознавание лиц в целях и способами, нарушающими стандарты в области прав человека.
- **Отсутствие стандартов**: стандарты и лучшие практики внедрения распознавание лиц все еще разрабатываются.[121] Также звучат призывы к введению имеющего обязательную силу кодекса поведения.[122] Несмотря на отсутствие стандартов, распознавание лиц продолжает использоваться как в общественных, так и в коммерческих пространствах по всему миру. Этот опасный вакуум не может быть

заполнен призывами к **этическому использованию**: этические проблемы должны быть разрешены на основе адекватной нормативно-правовой базы, соответствующей международным нормам в области прав человека.[123]

- **Двойное назначение**: подавляющее большинство систем распознавания лиц, предлагаемых к продаже частными структурами, могут использоваться в целях, незаявленных их разработчиками и продавцами. Другими словами, открыты огромные возможности для злоупотреблений, риск которых еще выше в силу отсутствия систем законодательного регулирования, гарантирующих, что технологии не будут использоваться в незаявленных целях, и предусматривающих ответственность за нарушения и средства правовой защиты.
- **Несоответствие требованиям необходимости и соразмерности**: многие способы применения технологии распознавания лиц уже признаны несоответствующими требованиям необходимости и соразмерности. Среди прочего использование в школах с целью контроля доступа учеников в помещения было осуждено как органами, обеспечивающими защиту данных, так и судами.[124]

Реализация свободы выражения мнений и информации и технологии распознавания лиц

С точки зрения обеспечения свободы выражения мнений внедрение и использование технологии распознавания лиц создает следующие дополнительные проблемы.

- **Право на сохранение анонимности**: использование в общественных местах распознавания лиц, особенно в реальном времени, представляет собой очевидную проблему для сохранения анонимности. Оно ограничивает возможность анонимного перемещения и пользования услугами, а. также возможность оставаться незамеченным в целом. Критически важно защитить общественное пространство для реализации основных прав и свобод, в частности, права на свободу выражения мнений. В случае активного развертывания данной технологии, например, применительно к записям видеонаблюдения или камерам, которыми снабжены полицейские, технология распознавания лиц может изменить природу общественного пространства.[125] Ее использование не проходит тест на необходимость и соразмерность. Нельзя допустить неизбирательное применение распознавания лиц, ведущее к массовой слежке в общественных местах.[126]
- **Право на выражение протеста**: использование технологий распознавания лиц во время протестов может удерживать людей от участия в них, что имеет явные негативные последствия для эффективного функционирования представительной демократии.[127]

Даже в случае насильственных протестов, распознавание лиц может затрагивать прохожих или тех протестующих, которые не предпринимают насильственных действий. Другими словами, использование распознавания лиц может вести к изменению людьми своего поведения и воздержанию от реализации права на протест. Таким образом, люди могут отказываться от встреч с другими людьми или организациями, участия в определенных мероприятиях или демонстрациях. Использование распознавания лиц в реальном времени в общественном пространстве может использоваться против журналистов, создавая неблагоприятные условия для свободы выражения мнений.

- **Свобода вероисповедания**: использования технологий распознавания лиц может препятствовать реализации свободы вероисповедания.[128] Такое может происходить, например, если людей обязуют открывать лица в общественных местах вопреки их религиозным традициям и вводят штрафы или предусматривают другие санкции в случае отказа.

Распознавание эмоций

Цели и применение технологий распознавания эмоций

Технология распознавания эмоций претендует на определение внутреннего эмоционального состояния человека на основании таких черт как движение мышц лица, тон голоса, движение тела и других биометрических сигналов. Она использует машинное обучение для анализа выражений лица и других биометрических данных с последующими выводами о эмоциональном состоянии человека. Такие технологии внедряются частными структурами среди прочего с целью адресной рекламы, привлечения внимания клиентов и воздействия на их выбор. По-видимому, они также являются крайне привлекательными для правительственных и правоохранительных органов, которые стремятся предвидеть противоправную деятельность, предотвратить террористические угрозы, а также осуществлять полицейскую деятельность в общественных, и все чаще – частных пространствах.[129]

Как и в случае других биометрических технологий, использование распознавания эмоций включает в себя массовый сбор конфиденциальных личных данных невидимыми и непрозрачными способами, что обеспечивает возможность отслеживания, контроля, категоризации, оценки или профилирования людей зачастую в режиме реального времени. Данные технологии используются в различных контекстах, таких как пограничный контроль или визуальное определение сотрудниками полиции «подозрительного поведения» или «террористов».[130] Государственные и частные структуры тестируют и внедряют эти технологии часто в сотрудничестве друг с другом, что ведет к значительным последствиям.[131]

Эффективность технологии распознавания эмоций

Два базовых допущения лежат в основе технологии распознавания эмоций: возможность оценки внутренних эмоций человека на основе внешности и поведения, а также дискретность и универсальность выражения внутренних эмоций по всему миру. Эта идея, известная как Теория базовых эмоций (ТБЭ), предполагает, что люди вне зависимости от их культуры могут уверенно различать эмоциональные состояния на основании выражений лица, которые, как утверждается, являются универсальными.[132] ТБЭ оказалась чрезвычайно влиятельной среди прочего вдохновив популярные телешоу и фильмы.[133] Однако в течение многих лет ученые расследуют, оспаривают и в значительной степени опровергают обоснованность этих утверждений, а также дискредитируют утверждение об универсальности выражения эмоций.[134]

Соответственно, технологии распознавания эмоций для идентификации, контроля, слежки и классификации людей в различных контекстах коренным образом проблематичны не потому, что они действительно работают, а потому, что заинтересованные стороны, создающие и использующие такие технологии, *заявляют*, что они работают.[135] Несмотря на это, научные исследования и прикладное применение продолжают строиться на допущении об универсальности выражения эмоций, вопреки сомнительным научным основаниям, связанным с давно опровергнутой расисткой псевдонаукой.[136]

Правозащитные проблемы, связанные с технологиями распознавания эмоций

Большая часть проблем, связанных с внедрением и использованием технологий распознавания эмоций, сходны с проблемами, упомянутыми выше, в связи с биометрическими технологиями и распознаванием лиц. Данные технологии также разрабатываются и внедряются невидимым, непрозрачным и ничем неограниченным образом в отсутствие механизмов надзора или общественного обсуждения. Кроме того, необходимо подчеркнуть нижеследующие проблемы:

- Технологии распознавания эмоций базируются на **ошибочных псевдонаучных основах и давно дискредитированных научных гипотезах**. Как было отмечено выше, они основываются на допущении, что выражение эмоций является универсальным, что эмоциональные состояния могут быть установлены на основе выражений лица, и что такие заключения являются достаточно надежными, чтобы служить основанием для принятия решений. Все три допущения десятилетиями опровергаются учеными по всему миру, но это, судя по всему, не препятствует разработке и продаже таких технологий. Хотя растет число технических проблем с технологиями распознавания эмоций, созданных коммерческими разработчиками, большая часть связана с техническими сложностями, с которыми сталкивается

сектор, осуществляющий слежку, при этом полностью игнорируются ложноположительные результаты и правозащитные последствия для тех, за кем следят эти технологии.[137]

Реализация свободы выражения мнений и технологии распознавания эмоций

Технологии распознавания эмоций создают сходные проблемы для реализации свободы выражения мнений, что и технологии распознавания лиц. Распознавание эмоций добавляет еще один уровень сложности и произвола, к и без того тревожной тенденции, с учетом отсутствия правовых оснований, гарантий и способности данной технологии особым образом вмешиваться в частную жизнь.

Заявления об определении «истинных» внутренних состояний людей с использованием распознавания эмоций и принятые на основе таких выводов решения способствуют представлению в качестве объективной реальности произвольных и односторонних допущений о людях. Это имеет два существенных последствия. Во-первых, применение данной технологии негативно влияет на реализацию права на свободу выражения мнений: осознание людьми того, что их не только видят и идентифицируют, но также оценивают и классифицируют, действует как механизм устрашения, вынуждающий их демонстрировать «одобренные» формы самовыражения, в противном случае их могут классифицировать как «подозрительных» или «представляющих угрозу». Во-вторых, с учетом широкого спектра применений, эти технологии могут сделать массовую слежку нормальным элементом повседневной жизни людей, особенно в гражданском пространстве. Важно отметить, что свобода выражения мнений включает в себя право не говорить и не выражать свое мнение.[138]

Природа данных технологий также несовместима с гарантиями человеческого достоинства. Они являются абсолютно излишним методом достижения декларируемых целей обеспечения национальной безопасности, общественного порядка и так далее. Хотя международные стандарты в области прав человека выделяют национальную безопасность и общественный порядок в качестве законных оправданий ограничения прав человека, включая свободу выражения мнений и неприкосновенность частной жизни, это не дает государствам свободу произвольно закупать и использовать технологии, воздействующих на реализацию прав человека без четких обоснований и веских причин.

Также очевидно отсутствие прозрачности деятельности государств и компаний по проектированию, разработке и использованию технологий распознавания эмоций. В то время как стимулы для разработки таких технологий предоставляются и стартапам, и известным технологическим компаниями,

в открытом доступе фактически невозможно найти обоснования органами власти покупки и содействия разработке таких продуктов, информацию о надзорных механизмах, правозащитных гарантиях в ходе проведения пилотных исследований и механизмах защиты данных. С учетом рисков, создаваемых технологиями распознавания эмоций для реализации прав человека, государства, которые их используют и закупают, обязаны обеспечить адекватную подотчетность, правовую определенность, процедурную и юридическую прозрачность их закупки и внедрения.[139] Компании также обязаны соблюдать требования прозрачности в соответствии с Руководящими принципами предпринимательской деятельности в контексте прав человека, которые требуют от компаний введения процедур защиты прав в случае нарушений, вызванных или усугубленных применением биометрических технологий.[140]

Рекомендации АРТИКЛЬ 19

Исходя из вышеизложенного, АРТИКЛЬ 19 предлагает заинтересованным сторонам принять подход к биометрическим технологиям, основанный на правах человека и учесть следующие рекомендации.

Важно отметить, что до реализации предложенных далее рекомендаций необходимо ввести **мораторий на разработку и внедрение данных технологий как государственными, так и частными структурами**.

Рекомендация 1. Массовая слежка с использованием биометрических данных должна быть запрещена

Государства должны запретить использование биометрических технологий в целях неизбирательной обработки биометрических данных в общественных и общедоступных пространствах онлайн и офлайн. Государства также должны прекратить финансирование программ и систем обработки биометрических данных, которые могут способствовать осуществлению массовой слежки в общественных пространствах.

Рекомендация 2. Необходимо запретить проектирование, разработку и использование технологий распознавания эмоций

Технологии распознавания эмоций по своей сути являются несовершенными и основываются на дискриминационных методах, оспариваемых исследователями в области эмоциональных вычислений и психологии. Они по своей природе не могут пройти четко сформулированный тест на необходимость, соразмерность, законность и легитимность. Соответственно, их разработка, продажа, передача и использование должны быть запрещены.

Необходимо ввести международные нормы, запрещающие подготовку концепций, проектирование, разработку, внедрение, продажу, экспорт и импорт таких технологий, отражая признание их принципиальной несовместимости с реализацией прав человека.

Рекомендация 3. Необходимо соблюдать принципы правомерности, соразмерности и необходимости при проектировании, разработке и использовании биометрических технологий

Государственные и частные структуры должны производить надлежащую оценку легитимности использования биометрических технологий для заявленной цели в каждом отдельном случае. Сама по себе доступность технологии никогда не должна становиться достаточной причиной для ее внедрения и использования. Проектирование, разработка и использовании этих технологий должны быть ограничены законными целями, соответствующими правозащитным стандартам и не унижающими человеческое достоинство.

Отправной точкой для оценки технологий, характеризующихся высокой степенью вмешательства в частную жизнь, таких как **распознавание лиц**, является признание того, что в силу этой присущей им характеристики такие технологии никогда не бывают безвредными. По этой причине государства должны рассмотреть введение запрета по умолчанию на распознавание лиц, предусмотрев использование данной технологии в исключительных случаях, когда такое использование должно быть оправдано и привязано к конкретной цели.

Когда определена законная цель для использования биометрии, разработка и внедрение технологий должны проходить четко сформулированный тест на необходимость и пропорциональность: технология должна быть категорически необходима и должны отсутствовать средства достижения указанной цели, в меньшей степени вмешивающиеся в частную жизнь.

Государствам необходимо избегать широкого применения биометрических технологий, в особенности распознавания лиц, в общественных местах, поскольку это лишает их основополагающей роли в реализации права людей на самовыражение и участие в общественной жизни. Государствам крайне важно не допустить, чтобы слежка стала нормой, сохранить роль общественных пространств в функционировании демократии, и соответственно, гарантировать право сохранять анонимность, протестовать и выражать себя в таких пространствах.

Государства должны препятствовать использованию биометрических технологий в отношении лиц или групп, играющих значимую роль в защите демократических ценностей, например, журналистов и активистов.

Рекомендация 4. Государства должны ввести соответствующе законодательное регулирование проектирования, разработки и использования биометрических технологий

Для законного использования биометрических технологий, соответствующего тесту на необходимость и соразмерность, государства должны создать адекватную **законодательную базу**, регулирующую их разработку и внедрение, которая должна включать в себя по меньшей мере:

- правила сбора и хранения, обеспечивающие адекватную защиту биометрических данных и достаточные гарантии против нарушений безопасности;
- требования, касающиеся качества данных, используемых для тренировки технологий; обязательное проведение внутренних аудитов и проверки точности и отсутствия расовых предубеждений;
- обязательство проводить предварительную оценку воздействия на защиту данных и на соответствие правозащитным стандартам, подлежащую регулярному пересмотру;
- обязательство как со стороны разработчиков, так и со стороны пользователей, предупреждать и минимизировать риски; это обязательство должно быть сформулировано с учетом уровня выявленных рисков;
- имеющие обязательную силу правила использования технологий правоохранительными органами;
- конкретные положения для предотвращения двойного применений и расширения сферы применения биометрических технологий как государственными, так и частными структурами.

Более того, инструментарии регулирования биометрических технологий должен предусматривать наличие красных линий, то есть ограничений, которые нельзя преступать.

Рекомендация 5. Проектирование, разработка и использование биометрических технологий должны быть прозрачными и открытыми для общественного обсуждения

Поскольку биометрические технологии затрагивают все более значительное число важных общественных процессов и демократических ценностей, их проектирование, внедрение и разработка должны производиться после открытого общественного обсуждения. Крайне важно активное участие

в обсуждении коалиций организаций гражданского общества и сетей экспертов. Это поможет гарантировать защиту прав и свобод от экономических интересов, а также избежать использования государствами широко сформулированных соображений безопасности для превращения массовой слежки в норму.

Рекомендация 6. Необходимо ввести и обеспечить выполнение требований прозрачности работы данного технологического сектора

Государства должны оповещать о любом реализуемом и запланированном использовании и развертывании биометрических технологий. Также необходимо предусмотреть прямое обязательство проводить общественные слушания по таким вопросам как последствия для реализации прав человека, связанные с закупками таких технологий, а также эффективности применения технологий для достижения заявленных целей.

Государства должны обеспечить максимальный уровень прозрачности и общественного контроля за процедурой государственных закупок в ходе приобретения, разработки и внедрения биометрических технологий. Прозрачность должна включать в себя критерии для оценки предложений о поставках, условия государственно-частных партнерств, содержание государственных контрактов, регулярную публичную отчетность об одобрении тендерных документов, закупок и использовании поставленных технологий.

Государства должны обеспечить право доступа к информации, связанной с проектированием, разработкой и использованием биометрических технологий, в соответствии с международными стандартами. Государства должны рассматривать информацию, касающуюся биометрических технологий, как «открытую» в рамках реализации законов, обеспечивающих право на информацию, и предпринимать усилия для ее своевременной публикации, а также предоставлять информацию в ответ на запросы.

Государственные и частные структуры должны регулярно публиковать оценки воздействия на обеспечение безопасности данных, а также доклады об оценке рисков, совместно с описанием мер, предпринимаемых для снижения рисков и защиты прав человека. Публикация не должна являться формальной: она должна способствовать обратной связи и диалогу, а также предусматривать возможность учета отрицательных мнений.

Рекомендация 7. Необходимо гарантировать подотчетность и доступ к средствам правовой защиты

Законодательная база для разработки и внедрения биометрических технологий должна предусматривать четкие структуры подотчетности и меры независимого контроля. Государства должны регулировать участие частного сектора экономики в исследованиях и разработке, выводе на рынок, продаже, передаче и техническом обслуживании биометрических технологий, используемых для осуществления слежки, а также проведение комплексной юридической оценки для обеспечения прав человека и истории соблюдения компаниями прав человека.

Законодательная база также должна обеспечить доступ к средствам правовой защиты для тех, чьи права нарушены в рамках использования биометрических технологий.

Рекомендация 8. Частный сектор экономики должен проектировать, разрабатывать и внедрять биометрические системы в соответствии со стандартами в области прав человека

Компании, занимающиеся проектированием, разработкой, продажей, внедрением и развертыванием биометрических технологий должны:

- Обеспечить **соблюдение правозащитных стандартов и защиту прав человека**. Для этого они должны применять подход, ориентированный на интересы человека, а также проводить заблаговременную оценку воздействия технологий на реализацию прав;
- Учредить процедуры адекватной и **регулярной оценки рисков** для обнаружения угроз для прав и свобод человека, и, в особенности, права на неприкосновенность частной жизни и свободы выражения мнений, связанных с использованием биометрических технологий, и использовать подход, базирующийся на минимизации рисков.
- Предусмотреть **эффективные средства правовой защиты** в случае нарушения прав человека.

Источники

1 См., например, the Council of Europe, Directorate General Human Rights and the Rule of Law, Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Data (Совет Европы, Генеральная дирекция по правам человека и верховенству права. Доклад о реализации принципов Конвенции №108 о защите физических лиц при автоматизированной обработке персональных данных), январь 2014 г., стр. 44. Биометрические технологии второго поколения также включают в себя распознавание лица или удаленное распознавание по радужной оболочке глаза, антропометрию (измерение морфологии тела), или физиометрию (измерение функций организма, например, частота сердцебиений, кровяное давление и др.).

2 См., например, S. Hood, Biometric Marketing: What Is Biometric Technology and How Can Marketers Use It?, Hitsearch (С. Худ. Биометрический маркетинг: что такое биометрическая технология и как ею могут воспользоваться маркетологи), 15 октября 2018 г.

3 Ср., например, Supreme Court of Illinois, Rosenbach v. Six Flags Entertainment Corporation, 2019 IL 123186 (Верховный суд штата Иллинойс. Розенбах против Оператора парков развлечений «Шесть флагов»).

4 См., например, Panel of experts at the request of the European Commission, Ethics and data protection (Группа экспертов по запросу Европейской Комиссии, Этика и защита данных), 14 ноября 2018 г.

5 См., например, European Data Protection Supervisor, Opinion 4/2015, Towards a new digital ethics, data dignity and technology (Европейская инспекция по защите данных, Заключение 4/2015. К новой цифровой этике, гарантиям человеческого достоинства при обработке данных и использовании технологий), 11 сентября 2015 г.

6 См., например, Centre for Data and Ethics and Innovation, Interim report: Review into bias in algorithmic decision-making (Центр информационной этики и инноваций. Промежуточный доклад: Обзор дискриминации в алгоритмическом принятии решений), июль 2019 г.

7 Ср., например, Верховный комиссар ООН по правам человека, Практические рекомендации для создания и поддержания безопасных и благоприятных условий для деятельности гражданского общества, основанные на передовой практике и извлеченных уроках, A/HRC/32/20, 11 апреля 2016 г.

8 В Китае, например, государство использует приложение для контроля доступа в общественные места, передающее данные полиции: см. New York Times, In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags (В ходе борьбы с коронавирусом Китай присвоил гражданам цветовые коды с предупреждающими знаками) 1 марта 2020 г. В Великобритании правительство планировало добавить возможность распознавания лиц в приложение, созданное при финансировании Национальной службы здравоохранения, для выявления контактов в целях эпидемиологического расследования, а также объявило, что распознавание лиц может использоваться при выдаче иммунных паспортов: см., например, The Telegraph, NHS app adds face-scanning sign ups in step towards immunity certificates (Национальная служба здравоохранения начала

использовать сканирование лиц как шаг в направлении введения сертификатов иммунитета), 19 мая 2020 г. В Лихтенштейне часть населения в настоящее время носит электронные браслеты, отслеживающие температуру кожи, частоту дыхания и пульса и другие биометрические данные. Правительство планирует расширить использование браслетов по всей стране к осени: см., например, L. Cendrowicz, Coronavirus Testing: Liechtenstein tracks virus with pioneering biometric bracelets, iNews.co.uk (Л. Цендрович, Тестирование на коронавирус: Лихтенштейн отслеживает вирус с использованием передовых биометрических браслетов), 16 апреля 2020 г.

9 См., например, New Statesman, Facial verification tech in NHS app could pave way for immunity passports (Технология верификации лиц в приложении Национальной службы здравоохранения может подготовит почву для иммунных паспортов), 20 мая 2020 г.

10 В настоящий момент использование таких наблюдательных шлемов подтверждено в Китае, Дубае и Италии: см., например, Business Insider, Police in China, Dubai, and Italy are using these surveillance helmets to scan people for COVID-19 fever as they walk past and it may be our future normal (Полиция в Китае, Дубае и Италии используют такие наблюдательные шлемы для сканирования прохожих на наличие температуры, типичной для COVID-19, что может стать нормой в нашем будущем), 17 мая 2020 г.

11 Более подробное обсуждение данной темы см., например, V. Marda, Papering over the crack: on privacy versus health, in Data Justice and Covid-19: Global Perspectives (В. Марда. Закрывая глаза на проблему: о противопоставлении неприкосновенности частной жизни и охраны здоровья. // Справедливость в сфере использования данных и Covid-19: глобальные перспективы), 2020.

12 См., например, Directive (EU) 2016/680 of the European Parliament and of the Council (Директива (ЕС) № 2016/680 Парламента и Совета Европейского Союза) от 27 апреля 2016 г. о защите физических лиц в отношении обработки их персональных данных компетентными органами в целях предотвращения, расследования, раскрытия или судебного преследования за совершение уголовных преступлений или исполнение уголовных наказаний, и свободной передачи таких данных, упраздняющая Рамочное решение Совета 2008/977/JHA (Директива о правоохранительных действиях), Статья 3 (13); Regulation (EU) 2016/679 of the European Parliament and of the Council (Регламент № 2016/679 Парламента и Совета Европейского Союза) от 27 апреля 2016 г. о защите физических лиц в отношении обработки их персональных данных и свободной передачи таких данных, и упраздняющий Директиву 95/46/ЕС (Общий регламент ЕС о защите данных), Статья 4(14); Regulation (EU) 2018/1725 of the European Parliament and of the Council (Регламент (ЕС) № 2018/1725 Парламента и Совета ЕС) от 23 октября 2018 г. о защите физических лиц в ходе их обработки институтами, органами, службами и агентствами Союза и о свободной передаче таких данных, упраздняющий Регламент (ЕС) № 45/2001 и Decision No 1247/2002/EC (Решение № 1247/2002/ЕС), Статья 3(18).

13 См., например, Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies (Рабочая группа по защите данных, учрежденная на основании Статьи 29, Заключение 3/2012 о развитии биометрических технологий).

14 См., например, D. Hambling, The Pentagon has a laser that can identify people from a distance-by their heartbeat, MIT Technology Review (Д; Хэмблинг. У пентагона есть лазер, который на расстоянии может идентифицировать людей по их сердцебиению), 27 июня 2019 г.

15 См., например, E. Mordini & D. Tzovaras (Eds.), Second Generation Biometrics: The Ethical, Legal and Social Context, Springer Netherlands (Е. Мордини и Д. Тцоварас (Ред.) Биометрия второго поколения: этический правовой и социальный контекст), 2019 г.

16 См., например, Article 29 Working Party, Opinion 02/2012 on facial recognition in online and mobile services, 00727/12/EN, WP 192 (Рабочая группа по защите данных, учрежденная на основании Статьи 29, Заключение 02/2012 о распознавание лиц онлайн и мобильными сервисами, 00727/12/EN, WP 192), Брюссель, 22 марта 2012 г., стр. 2.

17 АРТИКЛЬ 19, Emotional Entanglement: Freedom of expression Implications of China's Emotional Recognition Market (Эмоциональные затруднения: последствия рынка технологий распознавания эмоций в Китае для свободы выражения мнения), 2020 г.

18 См., например, Association for Psychological Science, Corrigendum: Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements (Ассоциация психологов. Исправление: Пересмотр выражения эмоций: вызовы определения эмоций на основе движений лица) 2016 г.; либо L. Feldman Barrett et al., Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements (Л. Фелдман Барретт и др. Пересмотр выражения эмоций: вызовы определения эмоций на основе движений лица) Psychological Science in the Public Interest. Volume 20, Issue 1, 2019 г.

19 См., например, A. Korte, Facial recognition technology cannot read emotions, scientists say (А. Корте. Ученые заявляют, что технология распознавания лиц не может распознавать эмоции) American Association for the Advancement of Science, 16 февраля 2020 г.; либо S. Porter, Secrets and Lies: Involuntary Leakage in Deceptive Facial Expressions as a Function of Emotional Intensity (С. Портер. Секреты и ложь: непроизвольная утечка в случае обманчивых выражений лица, связанная с сильными эмоциями как функция), Journal of Nonverbal Behavior, 36(1):23-37, март 2012 г.

20 См., например, A. M'charek, Tentacular Faces: Race and the Return of the Phenotype in Forensic Identification (А. М'чарек. Лица со щупальцами: раса и возвращение к использованию фенотипа в судебной идентификации), American Anthropologist, 6 мая 2020 г.

21 См., например, R. Wevers, Unmasking biometrics' biases: Facing gender, race, class and ability in biometric data collection (Р. Веверс. Разоблачение биометрических предубеждений: лицом к лицу с гендером, расой, классом и возможностями) Tijdschrift voor Mediageschiedenis 21.2 (2018): 89-105, TMG Journal for Media History.

22 Обзор данной темы см., например, в S. Fussel, An Algorithm That 'Predicts' Criminality Based on a Face Sparks a Furor, Wired (С. Фуссель. Алгоритм, «предсказывающий» преступность на основе лиц, вызывал негодование), 24 июня 2020 г.; K. Amjad & A.A. Malik, A Technique and Architectural Design for Criminal Detection based on Lombroso Theory Using Deep Learning (К Амжад и А.А. Малик. Техническое и архитектурное проектирование раскрытия преступлений на основании теории Ломброзо с использованием глубокого обучения), LGURJCSIT Vol. 4 No 3 (2020).

23 См., например, INTERPOL, Biometrics for Frontline Policing (ИНТЕРПОЛ. Биометрия для передовой полицейской службы); либо The Brussels Times, The Brussels Airport to be equipped with facial recognition cameras (Аэропорт Брюсселя будет оборудован камерами с технологий распознавания лиц), 9 июля 2019 г.

24 См., например, система идентификации граждан и резидентов Индии (Aadhaar),

национальная система удостоверений личности в ЮАР, система платежей PYMNTs; либо Deep Dive: Digital ID Developments From Around The World (Тщательный анализ: Развитие цифровой идентификации по всему миру), 27 февраля 2019 г.

25 Ср., Metropolitan Police and NPL, Metropolitan Police Service Live Facial Recognition Trials (Служба столичной полиции и Национальная физическая лаборатория Великобритании. Испытание распознавания лиц в реальном времени Службой столичной полиции) февраль 2020 г.

26 См., например, V. Marda & S. Narayan, Data in New Delhi's predictive policing system (В. Марда и С. Наранян. Данные в системе прогностической деятельности полиции Нью-Дели). 2020 г.; либо A. Daly, Algorithmic oppression with Chinese characteristics: AI against Xinjiang's Uyghurs (А. Дели. Алгоритмическое угнетение с китайскими характеристиками: искусственный интеллект против уйгуров в Синьцзяне), 2019 г.

27 Рост использования биометрии государствами для оказания государственных услуг и риск такого подхода был отмечен Специальным докладчиком ООН по вопросу о крайней нищете и правах человека в Докладе Генеральной Ассамблее в 2019 г.: см. Специальный докладчик ООН по вопросу о крайней нищете, Цифровые технологии, социальная защита и права человека, A/74/493, октябрь 2019 г.

28 См., например, использование биометрии при регистрации избирателей разработчиком биометрических технологий Thales; согласно вебсайту компании, в число таких стран входят Демократическая Республика Конго, Габон, Оман, Буркина-Фасо, Бенин, Филиппины и Швеция.

29 Ср., например, решение Верховного суда штата Иллинойс, указ. соч.

30 Сходные замечания были сделаны Специальным докладчиком ООН по вопросу о крайней нищете, указ. соч.

31 В силу принятия в форме резолюции Генеральной Ассамблеи ООН Всеобщая декларация прав человека не имеет юридически обязательный характер. Однако признано, что многие ее положения приобрели юридическую силу в качестве обычного международного права с момента ее принятия в 1948 г.: см. US Circuit Court of Appeals, 2nd circuit *Filartiga v. Pena-Irala*, 630 F. 2d 876 (1980) (Апелляционный суд второго округа США, Филартига против Пенья-Ирала).

32 Генеральная Ассамблея ООН. Международный пакт о гражданских и политических правах, 16 декабря 1966 г., Сборник международных договоров ООН, т. 999, стр. 171.

33 Статья 10 Европейской конвенции по правам человека (ЕКПЧ), 4 сентября 1950 г; Статья 9 Африканской хартии прав человека и народов (Банжульская или Африканская Хартия), 27 июня 1981 г.; Статья 13 Американской конвенции о правах человека (Американская конвенция), 22 ноября 1969 г.; и Статья 11 Хартии ЕС по правам человека (Хартия ЕС).

34 КПЧ ООН, Belichkin v. Belarus (Беличкин против Белоруссии), Comm. No. 1022/2001, UN Doc. CCPR/C/85/D/1022/2001 (2005).

35 КПЧ ООН, Замечание общего порядка №34, Статья 19: Свобода мнений и их выражения, CCPR/C/GC/34, параграф 18.

36 Там же, параграф 19. Те же формулировки повторяются в региональных правозащитных конвенциях, прежде всего в Статье 13 Американской конвенции, Статье 9 Африканской Хартии, Статье 10 ЕКПЧ и Статье 23 Декларации прав человека АСЕАН.

37 Международная конвенция о ликвидации всех форм расовой дискриминации, 21 декабря 1965 г., Сборник международных договоров ООН, т. 660, стр. 195.

38 Статья 11 ЕКПЧ, Статья 12 Хартии ЕС, Статья 15 Американской конвенции и Статья 11 Африканской Хартии.

39 КПЧ ООН, Замечание общего порядка № 37, Статья 21: право на мирные собрания, CCPR/C/GC/37, 27 июля 2020 г., параграф 36.

40 Статья 11 Американской Конвенции и Статья 8 Европейской Конвенции.

41 Ср., КПЧ ООН, Замечание общего порядка № 16: Статья 17 (Право на неприкосновенность частной жизни), Право на защиту от вмешательства в личную или семейную жизнь, посягательств на неприкосновенность жилища и корреспонденции, защиту чести и репутации, 8 апреля 1988 г., параграф 3; Международные принципы по соблюдению прав человека при использовании слежки в коммуникациях, или Принципы необходимости и соразмерности), Принцип 1.

42 ЕКПЧ, там же, Статья 14; Хартия ЕС, там же, Статья 21; Африканская Хартия, там же, Статьи 2 и 3; Американская конвенция, там же, Статья 24.

43 МПГПП, Статья 26.

44 Ср., например, АРТИКЛЬ 19, The Global Principles on Protection of Freedom of Expression and Privacy (Общие принципы защиты свободы выражения мнений и неприкосновенности частной жизни), 2017 г.

45 Замечание общего порядка № 16, указ. соч., параграф 10.

46 Руководящие принципы регламентации компьютеризированных картотек, содержащих данные личного характера, Резолюция ГА 45/95, 14 декабря 1990 г.

47 Конвенция о защите физических лиц при автоматизированной обработке персональных данных, ETS № 108.

48 В соответствии со Статьей 1 Хартии ЕС, человеческое достоинство является фундаментом всех основных прав, гарантированных Хартией. Соответственно, биометрические данные должны собираться и обрабатываться способом, который адекватным образом защищает человеческое достоинство: ср. также Европейский суд справедливости, C-377/98, Netherlands v. European Parliament and Council (Нидерланды против Парламента и Совета Европейского Союза), 9 октября 2001 г., параграфы 70-77. Кроме того, согласно Статье 52 (1) Хартии ЕС, всякое ограничение основных прав должно: (i) быть предусмотрено законом. Данное положение предусматривает исполнение соответствующей правовой базой качественного требования: норма должна быть публичной, точной и предсказуемой; (ii) подлинным образом соответствовать целям, представляющим общественный интерес, признанным Союзом, либо необходимости защищать права и свободы третьих лиц; (iii) уважать суть права; (iv) являться необходимой и соразмерной. Европейская инспекция по защите данных опубликовала строгие рекомендации относительно демонстрации необходимости и соразмерности. Агентство по основным правам (АПП) считает, что использование распознавания лиц может унижать человеческое достоинство, вынуждая людей отказываться от нахождения в общественных местах и участия в мероприятиях из-за чрезмерно жестких/насильственных способов сбора таких данных и «неподобающего поведения полиции»: см., например, Fundamental Rights Agency (FRA), Facial recognition technology: fundamental rights considerations in the context of law enforcement (АПП. Технология распознавания лиц: соображения, касающиеся основных прав в контексте правоохранительной деятельности), Вена, 2020 г., стр. 20.

49 African Union Convention on Cyber Security and Personal Data Protection (Конвенция Африканского союза о кибербезопасности и защите персональных данных), 2014 г. По мнению АРТИКЛЬ 19, уголовное наказание и регулирование на базе содержания, согласно Конвенции, не выполняют требований к допустимым ограничениям на свободу выражения мнений в соответствии с другими имеющими обязательную силу договоров правах человека.

50 OAS, Principles for Privacy and Personal Data Protection in the Americas (ОАГ. Принципы защиты неприкосновенности частной жизни и персональных данных в Америке), 2015 г., в настоящее время пересматриваются. Пересмотренные положения включают в себя прямое упоминание биометрических данных.

51 КПЧ ООН, Замечание общего порядка № 16 (Статья 17 МПГПП), 8 апреля 1988 г., параграф 10; где КПЧ ООН отметил, что данное право является необходимым для обеспечения права на неприкосновенность частной жизни.

52 Там же.

53 Ср., ЕСПЧ, *Gaskin v. the United Kingdom* (Гаскин против Соединенного Королевства), 7 b.kz 1989 г, Серия A № 160, параграф 49; *M.G. v. the United Kingdom* (М. Дж. против Соединенного Королевства), App. No. 39393/98, 24 сентября 2002 г., параграф 27; *Odièvre v. France* [GC] (Одьевр против Франции), App. No. 42326/98, ECHR 2003III), параграфы 41-47; *Guerra and Others v. Italy* (Герра и др. против Италии), App. No. 14967/89, 19 февраля 1998 г.

54 Общий регламент ЕС по защите данных, указ. соч.

55 FRA, Opinions Biometrics (АПП. Заключение о биометрии), 2019 г.

56 См., например, Закон о конфиденциальности биометрической информации Штата Иллинойс, где указано, что «подавляющее большинство представителей общественности обеспокоены использованием биометрической информации, когда она связана с финансовой или другой персональной информацией»: Illinois Compiled Statutes 740 ILCS 14/1 Biometric Information Privacy Act, Sec 5 (d).

57 Специальный докладчик о свободе выражения мнений, Доклад об использовании средств шифрования, и анонимности и системе обеспечения прав человека, A/HRC/29/32, 22 май 2015 г.

58 СПЧ. Резолюция. Право на неприкосновенность частной жизни в цифровой век. UN Doc. A/HRC/RES/34/7, 23 марта 2017 г., параграф 2.

59 Совет Европы, Конвенция о защите физических лиц при автоматизированной обработке персональных данных, 28 января 1981 г., ETS 108.

60 Regulation (EU) 2016/679 of the European Parliament and of the Council (Регламент (ЕС) № 2016/679 Парламента и Совета Европейского Союза) от 27 апреля 2016 г. о защите физических лиц в связи с обработкой персональных данных и свободном обменен такими данными, упраздняющий Директиву 95/46/ЕС (Общий регламент ЕС по защите данных), Статья 9.

61 Ibero-American Data Protection Network (RIPD), Data Protection Standards of the Ibero-American States (Иберо-американская сеть защиты данных, Стандарты защиты данных Иберо-американских государств), Статьи 2.1(d) и 29.4.

62 African Union Convention on Cyber Security and Personal Data Protection (Конвенция о кибербезопасности и защите персональных данных Африканского Совета), Статья 10 часть 4 пункт (d).

63 Верховный Комиссар ООН по правам человека, Право на неприкосновенность частной жизни в цифровой век, A/HRC/39/29, 3 августа 2018 г., параграф 14.

64 Там же, параграф 61 c).

65 Доклад Специального докладчика по вопросу о праве на свободу мирных собраний и праве на свободу ассоциации, A/HRC/41/41 17 май 2019, параграф 57.

66 Biometric Update, Biometric Update, UN privacy rapporteur criticizes accuracy and proportionality of Wales police use of facial recognition (Специальный докладчик ООН по вопросу о праве на неприкосновенность частной жизни критикует точность и соразмерность использования полицией Уэльса распознавания лиц), 3 июля 2018 г.

67 OHCHR, UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools (УВКПЧ, Эксперт ООН призывает к введению незамедлительного моратория на продажу, передачу и использования средств наблюдения), 25 июня 2019 г.

68 ЕСПЧ, *S. and Marper v. the UK* [GC] (С. и Марпер против Соединенного королевства), App. №№ 30562/04 и 30566/04, 4 декабря 2008 г., параграфы 112 и 125.

69 Совбез ООН, Резолюция 2396 (2017).

70 2018 Addendum to the 2015 Madrid Guiding Principles (Дополнение 2018 г. к Мадридским руководящим принципам 2015 г.) Приложение к письму, датированному 28 декабря 2018 г., адресованному Президенту Совета Безопасности Председателем Комитета Совета Безопасности, учрежденного Резолюцией 1373 (2001) по борьбе с терроризмом.

71 ООН, Сборник практических рекомендаций по ответственному использованию биометрических данных и обмену ими в рамках борьбы с терроризмом, подготовлен Исполнительным директоратом Контртеррористического комитета Совета Безопасности ООН и Офисом по вопросам контртерроризма Контртеррористического центра ООН, 18 июня 2018 г.

72 Руководящие принципы предпринимательской деятельности в аспекте прав человека: Осуществление рамок ООН, касающихся «защиты, соблюдения и средств правовой защиты» (Принципы Рагги), A/HRC/17/31, 21 марта 2011 г., Приложение. Совет по правам человека ООН поддержал Руководящие принципы в рамках своей резолюции 17/4, A/HRC/RES/17/14, 16 июня 2011 г.

73 Руководящие принципы предпринимательской деятельности в аспекте прав человека: Осуществление рамок ООН, касающихся «защиты, соблюдения и средств правовой защиты», подготовленные Специальным представителем Генерального секретаря по вопросу о правах человека и транснациональных корпорациях и других предприятиях, Джоном Рагги, 7 апреля 2008 г., A/HRC/8/5A/HRC/17/31. Совет по правам человека ООН поддержал Руководящие принципы в рамках своей резолюции 17/4 от 16 июня 2011 г.

74 Там же, Принцип 15.

75 Некоторые компании пошли еще дальше, и начали разработку своих собственных руководств и лоббирование законодателей с целью их принятия: см., например, Vox, Jeff Bezos says Amazon is writing its own facial recognition laws to pitch to lawmakers (Джефф Безос заявил, что Amazon ведет подготовку собственного законопроекта по регулированию распознавания лиц, чтобы предложить на рассмотрение законодателям), 26 сентября 2019 г.

76 Специальный докладчик по вопросу о свободе выражения мнений, Доклад

Совету по правам человека о свободе выражения мнений, государствах и частном секторе в эпоху цифровых технологий, 2013, A/HRC/32/38, 11 мая 2016 г.

77 Google, Artificial Intelligence at Google: Our Principles (Искусственный интеллект в Google: наши принципы).

78 Общеевропейская база данных соискателей статуса беженца, European Asylum Dactyloscopy Database (Европейская дактилоскопическая база данных соискателей статуса беженцев, EURODAC) предназначена для хранения отпечатков пальцев всех людей, пересекающих границу ЕС. Однако была высказана обеспокоенность после объявления о том, что база данных будет открыта для правоохранительных органов и Европола в целях расследования террористической деятельности. Перепрофилирование базы данных для целей борьбы с терроризмом, а не для иммиграции еще более стереотипирует и стигматизирует и без того уязвимые группы людей: соискателей статуса беженца, спасающихся от преследований, напрямую связывают с террористическими нападениями: см. Statewatch and PICUM, Data protection, Immigration Enforcement and fundamental Rights: What's the EU's Regulations on Interoperability Mean for People with Irregular Status (Защита данных, обеспечение соблюдения иммиграционного законодательства и основные права: что регламенты ЕС о функциональной совместимости означают для людей с неурегулированным статусом).

79 С. и Марпер против Соединенного королевства, указ. соч., параграф 103.

80 Массовый сбор метаданных на уровне ЕС демонстрирует, каким образом государства собирают информацию в определенных целях (например, обнаружение террористов), но с течением времени охват расширяется и включает в себя ненасильственные преступления, такие как ограбления.

81 CNIL, Reconnaissance facial: pour un débat à la hauteur de enjeux Французское управление по защите данных. Распознавание лиц: обсуждение насущных проблем), 15 ноября 2019, стр. 6.

82 Ada Lovelace Institute and DataKind UK, Examining the Black Box: Tools for Assessing Algorithmic Systems (Изучить «черный ящик»: инструменты для оценки алгоритмических систем), 29 апреля 2020 г.

83 Например, британская компания Sthaler разработала биометрическую систему для аутентификации клиентов и обеспечения безопасности на музыкальных фестивалях. Система в настоящее время используется и в других целях: см., например, From Sthaler to FinGo.

84 См. German Data Ethics Commission, Opinion (Немецкая Комиссия по информационной этике. Заключение), октябрь 2019 г.

85 Административный трибунал Марселя, 27 февраля 2020 г, req. n. 1901249.

86 При соответствующих правовых и процедурных гарантиях целенаправленный перехват сообщений определенного лица – законное действие демократического правительства, которое может быть необходимо для предотвращения преступлений и беспорядков, а также для защиты национальной безопасности. Целенаправленная слежка может быть обоснована, когда она предусмотрена законом, необходима для достижения законной цели и соразмерна преследуемой цели: см., например, ЕСПЧ, *Klass and others v. Germany* (Класс и др. против Германии), App. No. 5029/71, 6 сентября 1978 г. ЕСПЧ использовал понятие «разумные основания ожидать соблюдение неприкосновенности частной жизни» – степень, в которой можно рассчитывать на обеспечение неприкосновенности частной жизни в публичном пространстве без слежки –

один из факторов, позволяющих определить, происходит ли нарушение права на неприкосновенность частной жизни, согласно позиции ЕКПЧ: см ЕСПЧ, *Copland vs the UK* (Копланд против Соединенного Королевства), App. Nos. 62617/00, 3 июля 2007 г., параграф 42. Сходным образом Европейский совет по защите данных (EDPB) в своем руководстве по обработке персональных данных с использованием видеоустройств заявляет, что люди «также могут рассчитывать на отсутствие контроля в общественных местах, которые, как правило, используются для восстановления работоспособности, отдыха и досуга, а также местах, где люди могут пребывать и/или общаться, такие как зоны отдыха, столики в ресторанах, парки, кинотеатры, фитнес-центры. В этих случаях интересы или права и свободы субъектов данных часто перевешивают законные интересы контролера: см. EDPB Guidelines 3/2019 on processing personal data through video devices (Руководство 3/2019 об обработке персональных данных с использованием видеоустройств), Версия 2.0, 29 января 2020 г.

87 См., например, P. Fussey & D. Murray, Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology (П. Фуссей и Д. Меррей. Независимый доклад об испытаниях Службой столичной полиции технологии распознавания лиц в реальном времени), University of Essex, Human Rights Centre, июль 2019 г., стр. 36 и сноска 87. См. также International Justice and Public Safety Network, Privacy Impact Assessment: Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field (Международная сеть правосудия и общественной безопасности. Оценка воздействия на неприкосновенность частной жизни: использование технологий распознавания лиц для идентификации субъектов в реальных условиях), 30 июня 2011 г., Документ p. 016632, где утверждается, что «использование распознавания лиц в целях слежки может создать крайнее неудобство, влиять на поведение людей и вести к самоцензуре и самоограничению». См. также доклад Верховного комиссара ООН по правам человека «Воздействие новых технологий на поощрение и защиту прав человека в контексте собраний, включая мирные протесты», A/HRC/44/24, стр. 34.

88 Ср., ЕСПЧ, *Szabó and Vissy v Hungary* (Забо и Висси против Венгрии), App nos. 37138/14, 12 января 2016 г., параграф 38. См, также Human Rights Watch & Pen International, With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law and American Democracy (Свобода наблюдать за всеми: как массовая слежка в США вредит журналистам, законности и американской демократии) июль 2014 г.; и Национальная комиссия по вопросам информации и свобод, доклад 2019 г., указ. соч. (Национальная комиссия по вопросам информации и свобод отметила, что при постоянном наблюдении и распознавании лиц в общественных местах обычное поведение начинает казаться подозрительным, например, солнечные очки, капюшон на голове или внимание к телефону или к тротуару под ногами).

89 См., например, Доклад АПП 2020 г., указ. соч., стр. 20; или London Policing Ethics Panel, Final Report on Live Facial Recognition, май 2019 г.

90 Surveillance and Human Rights (Слежка и права человека), там же, стр. 26.

91 См., например, The Indian Express, Delhi Police film protests, run its images through facial recognition software to screen crowd, 28 декабря 2019 г.; India Today, Amit Shah on Delhi riots probe: 1100 people identified using facial recognition tech, 300 came from UP, 11 марта 2020 г.

92 Surveillance and Human Rights (Слежка и права человека), там же, стр. 15.

93 См., например, the Committee on Standards in Public Life, Artificial Intelligence and Public Standards, Section 4.7: Impact Assessment (Комитет по стандартам публичной сферы. Искусственный интеллект и нормы публичной сферы. Раздел 4.7: Оценка воздействия) февраль 2020 г. Комитет отметил, что надлежащая подотчетность зависит от понимания органами государственной власти рисков, связанных с использованием систем искусственного интеллекта для последующей оценки принятых мер с целью смягчения последствий их внедрения.

94 В декабре 2020 г. Апелляционный суд девятого Округа США приветствовал аргументы заявителя о том, что запросы на доступ к информации с целью получения сводных данных необходимы для уравновешивания общественного интереса в понимании того, каким образом правительство использует биометрические и другие собранные им персональные данные без раскрытия исходных данных, которые зачастую являются частными или иным образом вмешиваются в неприкосновенность частной жизни: см. US Court of Appeals for the Ninth Circuit, The Center for Investigative Reporting v. United States Department of Justice (Центр журналистских расследований против Министерства юстиции США, No.18-17356D.C. No. 3:17-cv-06557-JSC, 3 декабря 2020 г. Также см., например, EPIC v. FBI- Next Generation Identification (Информационный центр по обеспечению конфиденциальности цифровой информации EPIC против ФБР – Идентификация нового поколения); and US Government Accountability Office, Facial Recognition Technology Report and Recommendations (Счетная палата США. Распознавание лиц: технический отчет и рекомендации), май 2016 г.

95 Например, в Великобритании Управление Уполномоченного по хранению и использованию биометрических материалов, в чьи обязанности входит независимый надзор за режимом, учрежденным Законом о защите свобод 2012 г., и руководство хранением и использованием образцов ДНК, профилей и отпечатков пальцев полицией Англии и Уэльса, что не входит в сферу применения Закона о свободе информации. Соответственно, Управление не обязано отвечать на запросы о доступе к информации. Более подробную информацию о мандате и полномочиях Уполномоченного см. вебсайт Управления.

96 Запросы на доступ к информации позволили получить критически важные данные о технологии распознавания лиц, в том числе процент ошибок, лицензионные соглашения между государственными органами и частными компаниями или информацию о передаче биометрических данных между различными агентствами для широкого ряда целей: см., например, опыт Информационного центра EPIC в США по оспариванию использования биометрических технологий различными органами государственной власти: EPIC FOIA: DHS Biometric Program (Информационный центр EPIC Закон о свободе информации: Биометрическая программа Министерства национальной безопасности). Запросы на доступ к информации также продемонстрировали неспособность органов государственной власти обеспечить аудит соблюдения конфиденциальности при использовании агентством распознавания лиц, либо адекватным образом протестировать точность технологий: см., например, U.S. Gov't Accountability Office, GAO-16-267, Facial Recognition Technology: FBI should better ensure privacy and accuracy (Счетная палата США. Технология распознавания лиц: ФБР должно обеспечить более высокий уровень надежности и неприкосновенности частной жизни), 2016 г.

97 Ср., the UK Biometrics and Forensics Ethics Group Principles (Принципы Группы по биометрической и криминалистической этике), 2020 г.

98 Действительно, системы верификации 1:1 также создают ряд проблем: см., например, Kak A., The State of Play and Open Questions for the Future, in Regulating Biometrics: Global Approaches and Urgent Questions (Как А. Положение дел и нерешенные вопросы регулирования биометрии: общие подходы и актуальные вопросы), сентябрь 2020 г.

99 См., например, Доклад АПП 2020 г., указ. соч.

100 См., например, Planet Biometrics, Met begins operational use of Live Facial Recognition (LFR) (Служба столичной полиции начинает эксплуатацию распознавания лиц в реальном времени), 24 января 2020 г.; EDRigram, Serbia: Unlawful facial recognition video surveillance in Belgrade (Сербия: Незаконное видеонаблюдения с использованием распознавания лиц в Белграде), 4 декабря 2019 г.; Human Rights Watch, Facial Recognition Deal in Kyrgyzstan Poses Risks to Rights (Договоренность об использовании распознавания лиц в Кыргызстане создает угрозу реализации прав человека), 15 ноября 2019 г.; или The Times of India, From protest to chai, facial recognition is creeping up on us (От протеста до чая: к нам подбирается распознавание лиц), 5 января 2020 г.; The Ken, Watch this space: New Bill could unleash facial recognition free for all (Следите: законопроект может разрешить бесконтрольное использование распознавания лиц), 11 февраля 2020 г.

101 Например, в Бразилии системы распознавания лиц применяются по меньшей мере с 2011 г., их использование в целях обеспечения безопасности было значительно расширено в 2019 г. прежде всего, во время Карнавала в сотрудничестве с частными агентами. На сегодняшний день более 40 городов страны применяют данную технологию. См., например, Le Monde Diplomatique Brasil, Reconhecimento facial: a banalização de uma tecnologia controversa (Распознавание лиц: банализация спорной технологии), 22 апреля 2020 г. Обзор использования технологий распознавания лиц в Бразилии: см. Instituto Igarape, Infográfico: Reconhecimento facial no Brasil (Инфографика: Распознавание лиц в Бразилии).

102 См., например, The Guardian, Facial recognition… coming to a supermarket near you (Распознавание лиц… скоро в ближайшем супермаркете) 4 августа 2019 г; Big Brother Watch, Co-op Facial Recognition Supermarkets Revealed (Расследование использования распознавания лиц кооперативными супермаркетами), 14 января 2021 г.

103 См., например, Instituto Brasileiro de Defensa do Consumidor, IDEC, IDEC quer saber como Hering usa dados de reconhecimento facial de clientes (Бразильский институт защиты потребителей, IDEC запрашивает каким образом Hering использует данные систем распознавания лиц своих клиентов), 6 марта 2019 г.

104 См., например, IDEC, Idec pede esclarecimento sobre coleta de dado facial em loja do Carrefour (IDEC запрашивает пояснения относительно сбор данных для системы распознавания лиц у магазина Карфур), 23 апреля 2019 г.

105 См., например, IDEC, Justiça impede uso de câmara que coleta dados faciais em metrô em SP (Органы судебной системы предотвратили использование камер, собирающих данные для опознавания по лицу в метро Сан-Паулу), 18 сентября 2018 г.

106 См., например, The Telegraph, Uber faces racism claim over facial recognition software (Uber предъявлен иск в связи с программой распознавания лиц), 23 апреля 2019 г.

107 Например, Huawei заложил распознавание лиц в основание проекта «Безопасный город», который компания пытается реализовать в различных городах

по всему миру с особым упором на африканские и азиатские регионы: см., например, CSIS, Watching Huawei's "Safe Cities", 4 ноября 2019 г.

108 Например, в 2019 г. Сан-Франциско запретил использование распознавания лиц правоохранительными органами: см., например, EFF, Stop Secret Surveillance Ordinance (05/06/2019) (Постановление о запрете тайной слежки) и The Guardian, San Francisco was right to ban facial recognition. Surveillance is a real danger (Запрет на распознавание лиц в Сан-Франциско – правильное решение. Слежка представляет собой реальную опасность), 30 мая 2019 г. Портленд в настоящее время обсуждает запрет, включающий в себя использование технологии государственными и частными структурами: см., например, Fast Company, Portland plans to propose the strictest facial recognition ban in the country (Портленд планирует внести на рассмотрение самый жесткий в стране запрет на использование распознавания лиц), 12 февраля 2019 г. В Великобритании Полицейская служба Шотландии сообщила, что пока не будет внедрять технологию распознавания лиц, поскольку она «непригодна для использования» в силу, среди прочего обеспокоенности, связанной с обеспечением прав человека и неприкосновенности частой жизни. Планы внедрения, первоначально назначенного на 2026 г., были отложены с целью проведения более широких консультаций относительно воздействия технологии: см., например, BBC, Facial recognition: 'No justification' for Police Scotland to use technology (Распознавание лиц: «отсутствуют основания» для использования данной технологии Полицейской службой Шотландии), 11 февраля 2020 г.

109 Например, IBM в письме Конгрессу США о реформировании системы обеспечения расовой справедливости заявила, что прекратит продажу программного обеспечения для распознавание лиц «общего назначения»: см. IBM CEO's Letter to Congress on Racial Justice Reform, 8 июня 2020 г. Amazon объявила годовой мораторий на использование полицией технологии Rekognition: см. Amazon, We are implementing a one-year moratorium on police use of Rekognition, 10 июня 2020 г. Microsoft пообещала не продавать правоохранительным органам свои технологии распознавания лиц: см., например, The Washington Post, Microsoft won't sell police its facial recognition technology, following similar moves from Amazon and IBM, 11 июня 2020 г.

110 См., например, New York Times, The Landlord Wants Facial Recognition in Its Rent-Stabilized Buildings. Why? (Владелец сдаваемых в аренду квартир готов использовать распознавание лиц в зданиях с регулируемой арендной платой. Почему?), 28 марта 2019 г.

111 Например, в Москве городская администрация использует технологию распознавания лиц для обеспечения соблюдения карантина дома или в гостинице теми, кто обязан соблюдать самоизоляцию: см., например, Reuters, Moscow deploys facial recognition technology for coronavirus quarantine, 21 февраля 2020 г. Китайские компании развертывают технологию распознавания лиц, которая может определять повышенную температуру в толпе или отмечать граждан без масок: см., например, The Guardian, 'The New Normal': China's excessive coronavirus public monitoring could be here to stay, 9 марта 2020 г. Великобритания рассматривает использование распознавания лиц при введении иммунных паспортов.

112 См., например, Facewatch, Facewatch launces facemask recognition upgrade (Facewatch запускает обновление для распознавания при ношении масок), 11 мая 2020 г.

113 Вызывает беспокойство то, что Европейская Комиссия, по-видимому,

поддерживает данный подход, поскольку она недавно присвоила «знак качества» технологии под названием Aware, разработанную базирующейся в Испании компанией Herta Security, которая обеспечивает системы видеоанализа, включая распознавание лиц и анализ поведения толпы в реальном времени, для использования в борьбе против следующей возможной вспышки коронавируса: см., например, Euractiv, Crowd monitoring facial recognition tech awarded seal of excellence, 19 июня 2020 г.

114 В начале 2019 г. сербский министр внутренних дел и начальник полиции объявили о размещении 1000 камер в 800 точках в Белграде. Общественность информировали, что эти камеры наблюдения будут снабжены программным обеспечением, распознающим лица и номерные знаки машин. Три организации гражданского общества опубликовали подробную оценку воздействия на защиту данных Министерства внутренних дел об использовании умного видеонаблюдения, в которой сделан вывод, что технология не соответствует формальным и материальным условиям, в соответствии с сербским Законом о защите персональных данных. Сербское Агентство по защите данных подтвердило данные выводы. Более подробную информацию см., например, в EDRigram, Serbia: Unlawful facial recognition video surveillance in Belgrade, 4 декабря 2019 г.

115 В феврале 2020 г. Facebook урегулировал коллективный иск в штате Иллинойс, в котором пользователи заявили, что система подписи фотографий компании, использовала технологию распознавания лиц для анализа их фотографий, а также создает и хранит «шаблоны лиц», не информируя пользователей и не запрашивая у них разрешения по состоянию на июнь 2011 г.: см., например, New York Times Facebook to Pay $550 Million to Settle Facial Recognition Suit, 29 января 2020 г. Сходным образом Clearview AI, приложение для распознавания лиц, было разработано и широко распространялась среди правоохранительных органов, основываясь на базе данных, в которую вошли 3 миллиарда изображений, незаконно изъятых у Facebook, Google и YouTube. Несколько жителей штата Иллинойс подали иск к компании за нарушение Закона штата о биометрической информации. В марте 2020 г. генеральный прокурор штата Вермонт подал иск против этой компании, в котором ее методы работы названы «беспринципными, неэтичными и противоречащими государственной политике»: см., например, Gizmodo, We Found Clearview AI's Shady Facial Recognition App, 27 февраля 2020 г.; или Vermont Attorney General Office, Attorney General Donovan Sues Clearview AI for Violations of Consumer Protection Act and Data Broker Law, 10 марта 2020 г.

116 См., например, Why you can't really consent to Facebook's Facial Recognition (Почему нельзя дать Facebook разрешение на использование распознавания лиц), 30 сентября 2019 г.; E. Selinger & W. Hartzog, The Inconsentability of Facial Surveillance (Невозможность согласия на использование слежки на базе распознавания лиц) 66 Loyola Law Review 101 (2019).

117 См., например, Национальный Институт стандартов и технологий NIST (NIST) Study Evaluates Effects of Race, Age, Sex on Face Recognition Software (Исследование дает оценку влиянию расы, возраста, пола на программное обеспечение для распознавания лиц), 19 декабря 2019 г.; D. Leslie, Understanding bias in facial recognition technologies (Понимая предубеждения свойственные технологиям по распознаванию лиц), Институт Алана Тюринга, 2020; A. Najibi, Racial Discrimination in Face Recognition (Расовая дискриминация в распознавании лиц), 24 октября 2020 г.

118 См., например, J. Buolamwini & T. Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification (Оттенки гендера: несоответствия в точности коммерческих систем гендерной классификации в отношении интерсекциональности), 2018 г. Также Национальный институт стандартов и технологий (NIST) недавно провел исследование для оценки точности программного обеспечения распознавания лиц в отношении людей различного пола, возраста и расового происхождения. Согласно их выводам, ответ зависит от алгоритма в основе системы, приложения, которое его использует, и введенных данных. Данное исследование установило, что большая часть алгоритмов распознавания лиц демонстрируют демографические дифференциалы. Дифференциал означает, что способность алгоритма сопоставить два изображения одного и того же человека зависит от демографических характеристик. Женщины афроамериканского происхождения оказались группой населения с самым высоким числом ложноположительных результатов. В целом неточные результаты чаще всего затрагивали представителей азиатской, афроамериканской и индейской демографических групп: см. NISTIT, Facial Recognition Vendor Test (FRVT) Part 3: Demographic Effects, 8280.

119 См., например, ACLU, Amazon's Facial Recognition Falsely Matched 28 Members of Congress With Mugshots, 26 июля 2018 г., где задокументировано, что система распознавания лиц, разработанная компанией Amazon неверно идентифицировала 28 членов Конгресса США из 535 прошедших опознание, как людей с судимостью, и среди них непропорционально большое число были чернокожими; University of Essex, Human Rights Centre, Independent Report on the London Metropolitan Police Service's Trial of Live Recognition Technology, июль 2019 г., где установлено, что примерно 80% соответствий были неверными в шести испытаниях в реальном времени, проведенных Службой столичной полиции Великобритании в лондонских районах Сохо, Ромфорд и Стратфорд; Stark, Facial Recognition is the Plutonium of AI, 17 апрель 2019 г., с предупреждением о том, что расовые предрассудки являются характеристикой технологий распознавания лиц, а не случайной ошибкой.

120 Там же, ACLU. Более того, сообщается по меньшей мере о трех случаях, когда чернокожие мужчины в США были незаконно арестованы из-за ошибочного распознавания лиц.: см., NBCNews, Man wrongfully arrested due to facial recognition software talks about 'humiliating' experience, 26 июня 2020 г.; The New York Times, Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match, 29 декабря 2020 г.; The New York Times, Wrongfully Accused by an Algorithm, 24 июня 2020 г.

121 Ср., например, Interpol, Facial Recognition (Интерпол, Распознавание лиц).

122 См., например, the UK Information Commissioner's Office, ICO investigation into how the police use facial recognition technology in public places (Управление уполномоченного по вопросам информации. Управление расследует использование полицией технологии распознавания лиц в общественных местах), 31 октября 2019 г.

123 См., например, ARTICLE 19, Governance with teeth: How human rights can strengthen FAT and ethics initiatives on artificial intelligence (Зубастое управление: как права человека могут усилить инициативы, направленные на обеспечение справедливости, подотчетности, прозрачности и этических принципов в сфере искусственного интеллекта), апрель 2019 г.; ARTICLE 19 and Privacy International, Privacy and freedom of expression in the age of artificial intelligence (Неприкосновенность частной жизни

и свобода выражения мнений в эпоху искусственного интеллекта), апрель 2018 г.

124 В 2019 г. CNIL, Французское управление по защите данных, осудило использование технологии распознавания лиц, с целью регулирования и контроля доступа детей в школу поскольку эта цель может быть достигнута методами, не посягающими на основополагающие права детей: см. CNIL, указ. соч. Несколько неправительственных организаций также осудили использование этой технологии распознавания лиц в школах: см., например, La Quadrature du Net, La Ligue des droits de l´Homme, CGT Educ'Action des Alpes-Maritimes et la Fédération de Conseils de parents d'élèves des écoles publique des Alpes-Maritimes, Reconnaissance facial dans les lycées: un recours pour faire barrage à la surveillance biométrique (Распознавание лиц в школах: ресурсы для блокировки использования биометрической слежки), 19 февраля 2019 г. См. также Административный Суд Марселя, 9-я палата, Решение от 27 февраля 2020 г. К тому же, французский магистрат, принимавший участие в рассмотрение сходного дела в Марселе, заявил в ходе слушания, что «Регион берется за молоток, чтобы убить муравья», что является прекрасным сравнением между принятой мерой (система распознавания лиц) и ее целью (контроль доступа учеников в школу). Сходным образом, школьники из различных школ в США выступили против использования распознавания лиц, и в ряде случаев это привело к отказу руководства школ от внедрения данной технологии. См., например, The Guardian, Ban this technology': students protest US universities' use of facial recognition, 3 марта 2020 г.

125 Гражданское общество по всему миру все громче заявляет о воздействии надзора с использованием распознавания лиц на анонимность и негативном влиянии на свободу выражения мнений. Например, в Австралии заместитель директора Совета по гражданским свободам Нового Южного Уэльса в контексте расследования парламентом штата внедрения систем сопоставления изображений лиц заявил, что «это несет настоящую угрозу анонимности. Но вызывает еще большую обеспокоенность сопутствующее негативное воздействие на свободу политической дискуссии, право на протест и право на инакомыслие. Мы считаем, что возможные последствия должны вызывать всеобщую обеспокоенность»: см. The Guardian, Facial image matching system risks 'chilling effect' on freedoms, rights groups say, 7 ноября 2018 г.

126 См., например, E. Denham, Information Commissioner, Blog: Live facial recognition technology – police forces need to slow down and justify its use (Е. Денхам, Уполномоченная по вопросам информации. Блог: Технология распознавания лиц в реальном времени – полиции необходимо притормозить и обосновать ее использование).

127 В качестве примера, Министерство внутренних дел Индии в феврале 2020 г. арестовало 1100 человек, принявших участие в мирных протестах, идентифицировав их с помощью распознавание лиц: см. India Today, Amit Shah on Delhi riots probe: 1100 people identified using facial recognition tech, 300 came from UP, там же.

128 Свобода вероисповедания гарантирована Статьей 18 Всеобщей декларацией прав человека и наделена юридической силой положениями Статьи 18 МПГПП, а также другими региональными и национальными правовыми актами.

129 Там же.

130 См., например, Программа SPOT Администрации транспортной безопасности США или европейская система iBorderCtrl (система искусственного интеллекта,

осуществляющая предварительный мониторинг, сканирующая лица путешественников на признаки обмана при ответах на вопросы сотрудников пограничного контроля, опробованная в Венгрии, Латвии и Греции). Критика наборов данных, ложноположительные результаты и вероятность дискриминации привели к отказу от их использования. См., например, Government Accountability Office, Aviation Security: TSA Should Limit Future Funding for Behavior Detection Activities, 14 ноября 2013 г.; Department of Homeland Security Office of Inspector General, TSA's Screening of Passengers by Observation Techniques, май 2013 г.; *ACLU vs. TSA*, 8 февраля 2017 г.; Ars Technica, TSA's got 94 signs to ID terrorists, but they're unproven by science, 13 ноября 2013 г.; The Intercept, Exclusive: TSA's Secret Behavior Checklist to Spot Terrorists, 27 марта 2015 г.; Ars Technica, The premature quest for AI-powered facial recognition to simplify screening, 2 июня 2017 г.; J. Sánchez-Monederoa & L. Dencik, The politics of deceptive borders: 'biomarkers of deceit' and the case of iBorderCtrl'; The Intercept, We Tested Europe's New Lie Detector for Travelers — and Immediately Triggered a False Positive, 26 июля 2019 г.

131 Например, китайская система распознавания эмоций Alpha Hawkeye используется органами власти на железнодорожной станции Иу для задержания «преступников»; государственная автомобилестроительная компания Chang'an Automobiles продает машины с детекторами эмоций и усталости; компания Hikvision сотрудничает с Центром образовательных технологий Ханчжоу (отвечающим за поставки образовательных технологий для начальных и средних школ города) под руководством Управления образования Ханчжоу.

132 См., например, P. Ekman, E. Richard Sorenson & W. V. Friesen, Pan-Cultural Elements in Facial Displays of Emotion (П. Экман, Е. Ричард Соренсон и У. В. Фризен. Панкультурные элементы в проявлении эмоций на лице) Science, 1969, Vol. 164, Issue 3875, стр. 86–88; P. Ekman, Universal Facial Expressions of Emotions (П. Экман. Универсальное выражение эмоций на лице), California Mental Health Research Digest, 8(4), 151–158, 1973; P. Ekman, Universals and Cultural Differences in Facial Expressions of Emotions (П. Экман, Универсалии и культурные различия выражения эмоций на лице). In Cole, J. (Ed.), Nebraska Symposium on Motivation (стр. 207-282), Lincoln, University of Nebraska Press, 1973.

133 См., например, A. L. Hoffman & L. Stark, Hard Feelings - Inside Out, Silicon Valley, and Why Technologizing Emotion and Memory Is a Dangerous Idea (А. Л. Хоффман и Л. Старк. Уязвленные чувства – «Головоломка», Кремневая долина и почему опасна технологизация эмоций и памяти), Los Angeles Review of Books, 11 сентября 2015 г.

134 См., например, J. A. Russel, Is there universal recognition of emotion from facial expression? A review of the cross-cultural studies (Дж. А. Рассел. Существует ли универсальное распознавание эмоций на основе выражений лица? Обзор кросскультурных исследований), Psychological Bulletin, 115(1), 102–141, 1994; L. Feldman Barrett et al, Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements (Л. Фелдман Барретт и др. Пересмотр выражения эмоций: сложности опознания эмоций на основе мимики человека). Psychological Science in the Public Interest, Vol. 20, Issue 1, 2019; Oxford Scholarship Online, Coherence between Emotions and Facial Expressions, The Science of Facial Expression, 2017; The New York Times, What Faces Can't Tell Us (О чем не расскажут лица) 28 февраля 2014 г.

135 См., например, A. Daub, The Return of the Face (А. Дауб. Возвращение лица), Longreads, октябрь 2018 г.

136 См., например, L. Safra, C. Chevallier, J. Grezes & N. Baumard, Tracking historical changes in trustworthiness using

machine learning analyses of facial cues in paintings (Л. Сафра, С. Шевалье, Дж. Грезес и Н. Баумард. Отслеживание исторических изменений надежности анализа выражений лиц портретов на основе машинного обучения). Nature Communications, 11, 4728, 2020; или Coalition for Critical Technology, Abolish the #TechToPrisonTimeline (Письмо с призывом не публиковать исследование о технологии прогнозирования преступлений), Medium, 23 июня 2020 г.

137 См., например, С. Кун, С. Жендонг и С Беибеи. Мгновенное постижение истины: применение психологии микровыражений при таможенном контроле пассажиров (на китайском языке), Журнал таможенного контроля и торговли, 2018(03), стр. 31, 33.

138 Ср., Замечание общего порядка № 34, указ. соч., параграф 10, где утверждается, что «все формы принуждения к тому, чтобы они придерживались или не придерживались какого-либо мнения, запрещены. Право на свободное выражение мнений включает в себя свободу не выражать свое мнение».

139 Доклад Верховного комиссара ООН по правам человека, Воздействие новых технологий на поощрение и защиты прав человека в контексте собраний, включая мирные протесты, 24 июня 2020 г., параграф 40.

140 Руководящие принципы предпринимательской деятельности в аспекте прав человека, указ. соч., стр. 15.

www.article19.org