НАУКА ЗА РУБЕЖОМ

Октябрь, 2021 (№ 102)

ПРОБЛЕМЫ
ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ
РАСПОЗНАВАНИЯ ЛИЦ

Наука за рубежом

№ 102, октябрь 2021

Ежемесячное аналитическое обозрение
Издается с 2011 г., индексируется в РИНЦ
Электронное издание:

www.issras.ru/global_science_review

DOI: <https://dx.doi.org/10.37437/2222517X-2021-102-7-1-41>

Редакционная коллегия:

Л. К. Пипия (руководитель проекта), В. С. Дорогокупец,
О. Е. Осипова, Н. В. Шашкова, В. А. Хохлова

**Рубрика «Информационные и телекоммуникационные технологии
и вычислительная техника»**

Авторы выпуска: **Л. К. Пипия, В. С. Дорогокупец**

Перевод: **В. С. Дорогокупец**

Выпускающее подразделение: **Сектор анализа зарубежной науки**

Редактор О. Е. Осипова

Компьютерная верстка: Н. В. Шашкова

Художник А. Н. Горностаева

Размещение в сети Интернет: К. В. Никитин, Н. В. Шашкова

СОДЕРЖАНИЕ

1. Общая характеристика технологий распознавания лиц	4
2. Вопросы законодательного обеспечения применения технологий FRT	16
3. Технологии распознавания лиц на практике	26
ПРИЛОЖЕНИЕ	37
Рис. 1. Схема компромисса между точностью и конфиденциальностью в технологии распознавания лиц	37
Рис. 2. Отдельные результаты исследования «Perpetual Line-Up»	37
Табл. 1. Примеры использования технологий распознавания лиц по степени согласия и схеме распознавания	38
Табл. 2. Некоторые направления политики регулирования программы технологий распознавания лиц по секторам и административным уровням	38
Табл. 3. Примеры федеральных законов, регулирующих сбор, использование и хранение личной информации	39

Технологии распознавания лиц предназначены для обнаружения и распознавания людей, когда их изображения фиксируются объективом камеры. С практической точки зрения существует множество вариантов применения этих технологий, прежде всего в сферах, связанных с безопасностью, например для служб пограничного контроля и следователей, работающих на месте преступления. Однако технологии распознавания лиц несут в себе риски злоупотребления. Во-первых, правозащитные группы и широкая общественность выражают обеспокоенность по поводу конфиденциальности полученных данных во время съемки. Во-вторых, возникают вопросы и о законности применения таких данных с вытекающей отсюда необходимостью четких законодательных границ сфер применения этих технологий. Следовательно, выявление проблем, связанных с конфиденциальностью, предотвратит и злоупотреблением технологиями распознавания лиц, на раннем этапе позволяет снизить соответствующие риски в будущем.

1. Общая характеристика технологий распознавания лиц

Подобно технологиям распознавания отпечатков пальцев и радужной оболочки глаз технологии распознавания лиц (Face recognition technologies – FRT) представляет собой тип биометрической системы идентификации, которая основывается на распознавании образов для сопоставления лиц, исходя из заданного набора данных. Другими словами, оцифрованная информация о теле человека (в данном случае о лице) извлекается из изображений или видео и связывается с другими изображениями лиц или с дополнительной биографической информацией. Эксперты RAND Corporation подготовили доклад, в котором представили результаты изучения проблем, которые возникают при работе систем FRT и которые связаны с конфиденциальностью и несовершенством разрабатываемого кода [1].

Во избежание неверных толкований следует пояснить, что в дальнейшем будет использоваться термин «точность» для обозначения способности технологий распознавания лиц сравнивать изображения и правильно идентифицировать человека. Именно такое определение

применяется в таксономии, на которую опираются американские государственные учреждения, тестирующие и внедряющие FRT. Специалисты пришли к выводу, что точность в работе технологий распознавания лиц складывается из нескольких аспектов:

- максимизация истинных положительных результатов, или правильных определений совпадений;
- минимизация ложных срабатываний, или неправильных определений совпадений;
- минимизация ложных отрицательных результатов, или невозможности идентифицировать совпадения.

Каждый из аспектов имеет последствия для конфиденциальности и предвзятости в отношении субъекта. Прежде всего специалисты обеспокоены потенциальными проблемами конфиденциальности и тем влиянием, которое она оказывает на точность FRT. На этом поле существуют два эвристических метода. Первый – когда субъект осведомлен о наличии технологии распознавания лиц и принимает саму идею ее использования, соглашаясь или не соглашаясь непосредственно сотрудничать. В случае если субъект знает, что его изображение зафиксировано, и соглашается сотрудничать, добровольно предоставляя информацию, то изображения будут отличаться хорошим качеством, потому что субъект стоит на месте и смотрит прямо в камеру. Если же при применении FRT субъекту не предоставляется возможности отказаться от фиксирования его изображения, то изображения, как правило, получаются не очень качественными, менее точными, так как субъект закрывает лицо или принимает позы, затрудняющие распознавание лица.

Второй эвристический метод относится к проверке подлинности лица и его идентификации. Проверка подлинности лица – это индивидуальное (т. е. всех и каждого) сравнение уже имеющегося изображения лица с изображением другого лица, личность которого следует установить.

Идентификация лица подразумевает поиск двух одинаковых наборов данных (один из них может находиться в уже заведенной базе данных или являться изображением, взятом из толпы). Поиск может осуществляться по схеме «один – много», когда лицо из одной базы данных ищется в другой аналогично поиску в базе данных отпечатков пальцев на совпадение с

отпечатками пальцев человека, только что заключенного под стражу. Или же поиск может проходить по схеме «много – много», когда любое число записей из одного набора данных разыскивается в другом наборе данных, например данных с камер наблюдения. В настоящем обзоре оба типа идентификации – «один – много» и «много – много» – будут относиться к единой схеме «некоторые – много», несмотря на то что производительность поиска может отличаться в зависимости от варианта использования по типам соответствия. Указанный выше параметр имеет прямое отношение к точности и предвзятости технологий распознавания лиц, поскольку алгоритмы индивидуальной идентификации в настоящее время более точны, чем алгоритмы идентификации «много – много».

Данные, представленные в табл. 1, помогают оценить влияние потенциальных ошибок на конфиденциальность и предвзятость. В частности, можно предположить, что индивидуальная проверка с согласия субъекта будет отличаться большей точностью, чем идентификация по схеме «некоторые – много» без согласия субъекта. Следовательно, эту двумерную классификацию можно использовать в качестве набора критериев для определения того, насколько высокоточной будет система FRT.

Следует сразу оговориться, что под личной информацией в настоящей работе подразумевается способность человека контролировать информацию о себе, важность которой (не только в отношении людей, но и целых стран) неоспорима. Согласно Декларации прав человека Организации Объединенных Наций¹, право на неприкосновенность частной жизни является неотъемлемым правом человека. Его защита может сыграть значимую роль в балансе сил между странами, и это право должно защищаться как часть гражданских свобод.

На практике концепцию «личной информации» трудно внедрить из-за сложившихся условий. Министерство национальной безопасности США,

¹ В настоящее время под «дымовой завесой» коронокризиса и «борьбы» с ним в мире наблюдается повсеместное нарушение основополагающих прав и свобод человека, закрепленных в этом документе в результате более чем 200-летней классовой борьбы, мировых войн и осуждения преступлений фашизма. Правительства стран, ВОЗ, Мировой банк, МВФ и стоящие за ними фармкомпании и мировые цифровые платформы несут всю полноту ответственности за нарушение этих прав, обнищание населения, деградацию социальной защиты и банкротство малых и средних предпринимателей.

например, отметило, что оно уполномочено собирать биометрическую информацию от заявителей на въезд в Соединенные Штаты, утверждающих, что они являются гражданами США, и путешественников (по программе безвизового въезда), въезжающих в США. Однако, согласно отчету Центра по вопросам личной информации и технологий при Правовом центре Джорджтаунского университета, Конгресс никогда четко не санкционировал сбор биометрических данных у американских граждан с использованием технологий распознавания лиц.

Желание оберегать свою личную информацию (в частности, это защита от слежки) может заставить людей изменить поведение. Отвечая на вопрос о личной информации, респонденты из США сообщают, что хотят ее защитить и обеспокоены вопросами конфиденциальности. Респонденты из Европейского союза, у которых больше недоверия к институтам (например, правительству, бизнесу), озабочены проблемами личной информации еще сильнее. Сообщения в новостях о слежке со стороны правительства в Соединенных Штатах могли оказать сдерживающее воздействие на выступления журналистов, поведение пользователей в Интернете и способы самовыражения граждан в религиозной сфере. Иными словами, таким способом стимулируется самоцензура граждан и сообществ. Исследования долгосрочных эффектов наблюдения показывают, что, хотя люди могут адаптироваться к инвазивному наблюдению, они считают его причиной своего раздражения, беспокойства и порой гнева. В одном исследовании испытуемые даже отказались от любимых занятий и увлечений, чтобы продемонстрировать некоторую форму контроля над той информацией, которую могли увидеть наблюдающие за ними лица. Более того, нет никаких гарантий, что наблюдение за людьми заставит их быть добропорядочными гражданами и предотвратит преступления. Например, эффективность применения видеонаблюдения в борьбе с преступностью во многом зависит от контекста.

Принимая во внимание обеспокоенность общественности по поводу сохранности личной информации и результатов наблюдения, получение согласия от граждан является важным фактором при определении того, как будут реализованы технологии распознавания лиц. Использование FRT в отношении людей, которые не согласились предоставить информацию о себе, может иметь негативные краткосрочные и долгосрочные послед-

ствия. Это может привести к менее точным или неверно истолкованным результатам, например включению субъекта в черный список лиц, которым отказано в некоторых правах (например, допуск к авиаперелетам). Учитывая, что собранная информация, как правило, не является общедоступной (например, государственные списки, запрещающие полеты, расчеты рисков по страхованию), люди, оказавшиеся среди «ложноположительных» фигурантов, могут не знать о причинах, по которым их внесли в черные списки. В итоге это лишает их возможности потребовать возмещения ущерба или воспользоваться механизмами защиты (такими как правовая система) для оспаривания и разрешения выявленных недоразумений.

Технологии распознавания лиц могут оказаться чрезвычайно полезными, например для обеспечения физического доступа к объекту или проезда через границу. При этом требуется согласие субъекта на фотосъемку, чтобы получить фотографию лица, которую можно было бы в дальнейшем использовать для сличения. Например, для некоторых поездок требуется паспорт; если кто-либо желает совершить поездку, но не дает согласие на оформление паспорта в связи с отказом фотографироваться или не предоставит фотографию, отвечающую требованиям для оформления паспорта, то его данные будут отсутствовать в паспортной базе данных и, следовательно, этому человеку будет отказано в поездке.

При развертывании новых технологий, особенно в контексте безопасности, правительственные агентства должны будут рассмотреть неизбежный компромисс между обеспечением безопасности и защитой конфиденциальной информации. В сфере обеспечения конфиденциальности, которая заметно выросла за последние годы, рассматриваются возможности встраивания защиты конфиденциальности в само программное и аппаратное обеспечение. Обеспечение конфиденциальности подразумевает применение множества инструментов и методов, но использование трех из них наиболее вероятно при внедрении системы FRT.

Во-первых, *защита данных* направлена на обеспечение безопасности существующих данных с помощью шифрования или разделения системных ролей или задач. Это гарантирует целостность данных и их доступность только для предполагаемых и авторизованных пользователей. Такая за-

щита особенно важна для предотвращения злонамеренных попыток сбора информации.

Во-вторых, *минимизация, сокращение и анонимность данных* предполагают снижение объема информации, доступной даже для авторизованных пользователей. Примеры подходящих методов включают дифференциальную конфиденциальность и k-анонимность². Каждый из этих методов направлен на то, чтобы скрыть идентифицирующую информацию о лицах в базе данных, обеспечивая при этом ее полезность для анализа. Дифференциальная конфиденциальность обеспечивает это путем добавления статистического «шума» к данным, в то время как k-анонимность объединяет данные в группы, в которых членов группы нельзя различить между собой.

В-третьих, *прозрачность и возможность скорректировать данные* представляют собой методы доступа и контроля, которые помогают субъектам (например, путешественникам) понять, как обрабатываются их данные. Сложные параметры доступа пользователей и управления конфиденциальностью включают предоставление общественности уведомления, которое помогает потенциальным субъектам понять, какая информация о них используется и как она используется, а также и выбор, позволяющий контролировать поток информации. Кроме того, должны быть доступны возможности для внесения поправок в информацию, если в этом возникнет необходимость. Несмотря на доступность уведомления и выбора, контроль отдельных лиц над своими данными в конечном итоге зависит от того, какую точку баланса между конфиденциальностью и безопасностью выберет государственное учреждение.

Первые две возможности (защита данных и минимизация, сокращение или анонимизация данных) находятся только в сфере контроля разработ-

² K-анонимность – это метод, с помощью которого можно скрыть персональную информацию нескольких лиц в наборе данных, если эти лица похожи друг на друга. Буква k определяет число лиц в группе. Считается, что набор данных обладает k-анонимностью, если для каждого лица в группе имеется по меньшей мере k – 1 лицо, обладающее такими же свойствами. Предположим, в наборе данных представлены почтовые индексы, а значение k равно 50. Если наугад выбрать любое лицо, то можно будет найти еще 49 человек с тем же почтовым индексом. Это значит, что найти в этой группе конкретное лицо только по почтовому индексу невозможно. – <https://policies.google.com/technologies/anonymization?hl=ru>

чиков системы и специалистов по ее внедрению. В этом случае у людей, чьи лица сравниваются, практически не будет возможности повлиять на конфиденциальность информации. Разработчики и изготовители системы должны обеспечивать транспарентность и возможность внесения поправок данных, и эти методы предоставляют больше возможностей для субъекта (например, путешественника), чтобы понять и исправить данные о себе.

Один из способов сохранить свою конфиденциальность – это «взломать» технологию распознавания лиц. FRT не защищены от попыток подорвать их эффективность с помощью различных атак. В зависимости от намерения того, кто совершает эти действия, они могут рассматриваться как средство защиты конфиденциальности, затрудняя сканирование камерами лица (предотвращение обнаружения), либо как действия, которые считаются противоправными – фальсификации черт лица (выдача себя за другого человека).

Предотвращение обнаружения, также известное как уклонение, или биометрическая обфускация³, может увеличить различия между физическим внешним видом субъектов и набором изображений, используемых для их идентификации. В настоящее время почти все варианты методов избежать обнаружения основываются на временном или постоянном изменении физических черт лица или их сокрытии. Временные методы, такие как использование социально приемлемых барьеров (например, шарфов) или накладных волос на лице (например, усов и бороды), могут ухудшить способность системы FRT обнаруживать искомую личность. Несколько исследований подчеркнули роль очков в предотвращении обнаружения. Субъекты, которые на опознавательных фотографиях носят очки, с большей вероятностью уклонятся от технологий распознавания лица после того как снимут их («эффект Кларка Кента»⁴). Очки также могут быть спроектированы таким образом, чтобы вводить в заблуждение FRT. Они могут производить определенные цветовые импульсы, создавая их из материалов, которые поглощают и отражают естественный свет различными

³ Обфускацией называется преднамеренное сокрытие программного кода путем его запутывания с сохранением работоспособности программы.

⁴ Эффект Кларка Кента – невозможность распознать человека благодаря такой мелочи, как очки, или другого атрибута или аксессуара. Назван по имени главного героя фильма «Супермен».

способами или путем излучения инфракрасного света, который ослепляет камеры. Недостатком светоизлучающего метода является то, что он может привлечь внимание, поскольку тот факт, что кто-то пытается избежать идентификации, сразу же станет подозрительным.

Применение временного или перманентного макияжа также может снизить эффективность технологий распознавания лица. Разработчики из Университета Западной Вирджинии и Национального университета Сингапура Гуодонг Гуо и его коллеги создали таксономию, описывающую, как нанесение макияжа создает контраст в чертах лица человека. Таксономия включает такие параметры, как оттенок цвета кожи, изменение которого может быть использовано для искажения видимых признаков распознавания расы человека, гладкость и текстура кожи, изменение которых может исказить внешний вид шрамов, прыщей и морщин, а также блики на коже, подчеркивающие различные элементы лица. Косметическая хирургия – это метод, навсегда изменяющий черты лица, который ставит под сомнение точность работы технологий распознавания. Изменения могут быть локальными (на одном элементе лица) или глобальными (полностью переделанное лицо). Способность правильно идентифицировать человека, который перенес пластическую операцию, может значительно варьироваться в зависимости от методологии FRT и типа операции. Например, частота успешной идентификации после отопластики (операции на ухе) колеблется примерно от 56 до 90%, в то время как показатели идентификации после пилинга кожи могут составлять от 5 до 95%.

Желание выдать себя за другое лицо или ввести других в заблуждение, применяя дезориентирующие помехи, т. е. сознательно уменьшая различия в лицах между одним человеком и другим, преследует определенную цель. В частности, цель может заключаться в том, чтобы получить доступ к системе или заставить поверить в то, что определенное лицо присутствует в нескольких местах одновременно. Хотя методы введения в заблуждение схожи с теми, что используются для предотвращения обнаружения, первые представляют собой более сложную задачу. В исследовании по этой теме описаны четыре метода подделки личности: при помощи фотографии, видео, маски и морфинга⁵.

⁵ Морфинг – технология в компьютерной анимации, визуальный эффект, создающий впечатление плавной трансформации одного объекта в другой. Используется в игровом и телевизионном кино, в телерекламе. Встречается в трехмерной и двухмерной (растровой и векторной) графике.

Фотография. Подделка фотографий – наиболее распространенный метод, поскольку он самый простой и недорогой. Для этого достаточно, чтобы субъект получил фотографию необходимого ему лица и предъявил ее системе FRT. К недостаткам такого подхода можно отнести отсутствие трехмерной информации и наличие вибраций, вызванных рукой, держащей изображение. Кроме того, фотография вряд ли будет имитировать определенные характеристики живого человека, такие как движение глаз и рта, известное в литературе как «живость лица». Один из методов борьбы с этим недостатком – вырезать отверстия для глаз и рта, что позволяет имитатору придать изображению «естественные» движения.

Видео. Качественное видео лица, показываемое на экране с высоким разрешением, является альтернативой фотографиям при выдаче себя за другое лицо. В отличие от фотографий, черты лица на видео вряд ли будут статичными. Если технологии распознавания лиц включают параметр «живости» в процесс идентификации личности, то видео, на котором человек моргает, делает мимические движения и дышит, является полезным средством проверки. Однако воспользоваться этими преимуществами можно лишь в том случае, когда черты лица видны очень четко.

Маски. Самая сложная техника дезориентации и создания помех в распознавании – это создание и представление трехмерной маски. Развитие технологий трехмерного сканирования и печати предоставило инструменты, облегчающие создание имитации лица для дезориентации системы FRT. Основная проблема, с которой сталкиваются имитаторы, заключается в том, что получение доступа к информации, необходимой для построения точного изображения, практически невозможно без сотрудничества имитируемого лица. Некоторые системы идентификации лица взаимодействуют с объектами и просят их сделать серию движений или движение, запрограммированное в качестве пароля, которые помогают выявить обман при помощи маски. Добавление других видов идентификации на основе биометрических данных (например, проверка походки или речи) в технологии распознавания, вероятно, помогут противостоять взлому системы.

Морфинг. Последний тип атаки известен как морфинг, при котором изображение одного человека сочетается с изображением другого, похожего на него, человека. Исследователи из Университета Йорка в Великобритании Робертсон, Крамер и Бертон предложили сценарий, в котором два

лица предоставляют обновленную информацию о себе (для идентификации государственными органами) с помощью своих трансформированных изображений, чтобы оба эти субъекта могли использовать новый документ. В предварительных тестах системы идентификации лица приняли измененные параметры как удовлетворительные в 68% случаев, в то время как системы распознавания, предлагающиеся на рынке (например, в мобильном телефоне), воспринимают морфинг только в 27% случаев.

Особую озабоченность – не только у разработчиков систем распознавания, но и у специалистов по машинному обучению – вызывают погрешности. Погрешности заключаются в неоправданных тенденциях, благоприятствующих (или неблагоприятствующих) одной группе по сравнению с другой. Особенное беспокойство вызывают незаконные, неэтичные и нежелательные предубеждения против определенных групп людей. Меньшинства и группы, которые считают, что они могут не идти в ногу с большинством или исследуемыми сообществами, не всегда заявляют о себе открыто. В системах FRT предвзятость может базироваться на физических характеристиках лица, таких как форма глаз или цвет кожи. Примеры алгоритмической предвзятости очень хорошо известны в различных областях, например в уголовном праве и в наблюдении за заболевшими. Предвзятые результаты систем распознавания могут нанести серьезный вред.

Учитывая, что технологии распознавания лиц обычно полагаются на алгоритмы, обученные на основе данных, чтобы сосредоточиться на конкретных характеристиках, различные конфигурации и операционные подходы могут непропорционально влиять на группы населения при совершении системой действий, рассчитанных на целевую аудиторию.

Методы контролируемого обучения, обычно используемые для программирования систем распознавания, основываются на данных, предварительно помеченных вручную. Именно так алгоритмы обучают тем характеристикам, на которых им следует сосредоточить свое внимание. Таким образом погрешности в обучающих данных (входных данных) могут привести к искажению выходных данных. Например, если набор фотографий лиц содержит непропорционально мало людей определенной расы или с определенными чертами лица, алгоритм FRT никогда не научится их распознавать.

Как показывают исследования, демографический перекося в данных по обучению может повлиять на способность FRT идентифицировать людей. В одном из таких анализов изучалась роль демографической информации в наборе доступных на рынке инструментов FRT. Результаты показали, что лица чернокожих молодых женщин постоянно определялись неверно. В частности, расовая предвзятость в FRT известна как «эффект другой расы», который заключается в том, что люди способны лучше узнавать лица своей расы. При сравнении алгоритмов, разработанных на основе обучающих данных из стран Западной или Восточной Азии, было обнаружено, что алгоритмы работают точнее по отношению к светлокожим лицам и лицам восточноазиатского типа. Отчеты показали, что многие системы FRT плохо распознают чернокожие лица. В другом исследовании ученые выявили, что три коммерческих системы распознавания, ориентированных на гендерную классификацию, такие как Microsoft Cognitive Services, IBM Watson и Face++, лучше всего подходят для мужчин и людей со светлой кожей. Эти FRT хуже всего работали с темнокожими женщинами. Авторы исследования также пришли к выводу, что несколько общедоступных наборов данных изображений лиц содержат непропорционально много светлокожих и гораздо меньше темнокожих лиц, в частности темнокожих женских лиц.

После обучения система распознавания применяется к целевым данным – набору данных о помеченных или идентифицированных изображениях лиц, среди которых, отталкиваясь от заданного изображения или набора изображений, FRT ищет потенциальные совпадения. Важным моментом является происхождение и, следовательно, состав этого набора данных. Например, набор данных о лицах может быть предназначен либо для составления целевой группы, представляющей интерес (например, подозреваемых преступников или террористов), либо для составления самого широкого круга лиц (например, кадры видеонаблюдения, фотографии с водительских удостоверений). Как это ни парадоксально, риск необъективных результатов может быть выше, если используются более ограниченные наборы справочных данных. Если, например, набор данных о лицах содержит снимки из архива арестованных лиц, расовая предвзятость в количестве арестованных может привести к искажению демографических данных в фотографиях. Это повысит вероятность того, что показатели совпадения лиц будут непропорционально высоки среди

расовых и этнических групп, которые непропорционально представлены в наборе справочных данных. В результате это нанесет вред как людям в чрезмерно представленной группе, подвергнув их неоправданной проверке, так и широкой общественности, для защиты которой предназначена система распознавания (например, связанная с безопасностью). Действительно, данные об одной целевой группе могут преобладать над данными о некоторых других группах. Например, базы данных фотографий задержанных полицией людей могут содержать непропорционально больше чернокожих лиц из-за непропорционально высокого числа арестов. Демографический состав несовпадающих изображений лиц в целевом наборе данных, иначе говоря «фон», на котором находятся совпадающие изображения, также может влиять на производительность алгоритма. Итак, точность FRT растет с увеличением количества обучающих данных и снижается по мере увеличения размера набора данных одной отдельно взятой целевой группы.

Системы распознавания лиц построены на алгоритмах, которые сравнивают изображения лиц и оценивают вероятность совпадений. Хотя такие компьютерные методы можно считать безошибочными или по крайней мере менее подверженными погрешностям, чем люди, на самом деле алгоритмы могут содержать скрытые предубеждения, которые отражают опыт, характеристики и даже предпочтения разработчиков, их создавших. Например, может быть написан алгоритм для присвоения чрезмерного веса, исключения или неверной интерпретации определенных характеристик данных в его модели. Более того, эти варианты могут быть совершенно неизвестны. Непреднамеренный или преднамеренный ущерб может возникнуть из-за непрозрачности алгоритмов или отсутствия прозрачности в отношении используемых для идентификации и сопоставления лиц функций.

Большая часть споров об обеспечении справедливости в системах FRT вращается вокруг устранения непреднамеренной предвзятости. Однако алгоритмы или наборы данных могут проявлять предвзятость преднамеренно, будучи разработанными таким образом, чтобы результаты коррелировали с расой. В качестве примера можем привести случай, выявленный при найме на работу. Сотрудников искали на основе алгоритма, вычисляющего расстояние от дома сотрудника до работы. С одной стороны, такое деление, казалось бы, совсем безобидно, с другой, если учесть

существующую в США сегрегацию населения по районам, такой отбор приобретает оттенки предвзятости. Подобные алгоритмы, используемые для систем распознавания лиц, могут исказить результаты в сторону непропорционального включения или исключения определенных групп, например, для продвижения идеологии или использования политической поляризации с целью дестабилизации общества.

Абсолютно все технологические системы, внедряемые в целях безопасности, должны оцениваться на предмет конфиденциальности и предвзятости, включая системы распознавания лиц. Потенциальные проблемы в вопросах конфиденциальности при заданных условиях и предполагаемые уровни точности, которые включают в себя возможность предвзятости (большее число ложных ответов снижает точность), представлены на рис. 1. Например, когда лицо субъекта сравнивается при его согласии с фотографией в паспорте, точность, как правило, должна быть высокой, а вероятность нарушения конфиденциальности должна быть низкой.

2. Вопросы законодательного обеспечения применения технологий FRT

В этой части обзора рассматриваются отдельные направления государственной политики и законы, которые ограничивают или регулируют использование технологий распознавания лиц. При этом следует учитывать, что описание некоторых программ и приложений систем FRT, на которые влияет эта политика, представлено очень кратко, лишь для того, чтобы показать существенные причины, которыми руководствуются при определении порядка использования технологий распознавания, особенно на разных административных уровнях или в различных секторах. Приведенная здесь информация не является исчерпывающим описанием каждой государственной программы или политики, относящейся к FRT. Скорее, это совокупность секторов, в которых такие технологии применяются для идентификации или наблюдения за людьми. В табл. 2 представлена юрисдикция различных административных уровней в отношении рассматриваемых здесь секторов: школы, правоохранительные органы, частный сектор и национальная безопасность.

Школы

После инцидентов с насилием в школах по всей территории США местные округа рассмотрели возможность установки систем FRT для усиления безопасности персонала и учащихся. Такие системы варьируются по целевому назначению. Это может быть система слежения за входящими в здание взрослыми (сопоставление по схеме «один – много») или предупреждение администраторов о присутствии людей, которые могут представлять опасность (сопоставление «некоторые – много»). В частности, последняя схема предназначена для идентификации людей в наборах данных о сексуальных преступниках, исключенных студентах и бывших сотрудниках. В качестве дополнительного преимущества, которое не связано с распознаванием лиц как таковым, некоторые системы также способны обнаруживать наличие оружия.

RealNetworks SAFR – система безопасного и точного распознавания лиц, которая была протестирована по схеме «один – много». Эта программа в настоящее время внедряется в одной из школ Сиэтла, где работает на имеющемся в наличии оборудовании, проверяя личности учителей и родителей, которые принимают участие в программе. Разработчик не предоставляет информации о точности своего программного обеспечения, и все соображения относительно безопасности, конфиденциальности и согласия обработки данных, собранных от участников, оставлены на усмотрение школы.

Другие подходы не предусматривают механизм согласия. Некоторые школы либо планируют, либо уже установили систему FRT «много – много». Например, в своем последнем Генеральном плане безопасности Независимый школьный округ Форт-Бенд в Техасе предлагает внедрить систему, которая будет выявлять лиц, получивших несанкционированный доступ на территорию кампуса, и оповещать об этом учащихся и сотрудников через специальное мобильное приложение. Округ Нью-Йорка, Локпорт-Сити за счет государственного гранта в размере 4 млн долл. закупил 300 камер и оборудование с функцией FRT для восьми школ, которые предназначены для предупреждения властей округа об обнаружении среди любого из множества наборов данных человека с разрешением на ношение оружия. Власти Локпорт-Сити утверждали, что такая система повысит безопасность и полезность существующей инфраструктуры камер, потому что ранее система наблюдения использовалась только для просмотра событий после того, как они произошли. Совет школы «Магнолия» в Арканзасе приобрел

более 200 камер за 300 тыс. долл., чтобы внедрить систему аналогичную системе в Локпорт-Сити.

Что касается вопросов конфиденциальности и безопасности данных, то каждый школьный округ сам решает, как использовать систему FRT. В случае с Локпорт-Сити департамент образования штата Нью-Йорк одобрил использование системы FRT и заверил общественность, что данные не будут передаваться третьим лицам, а все собранные видео подпадут под правила хранения и использования данных, действующие на территории школьного округа. Группы, которые следят за гражданскими свободами и правами, такие как Американский союз гражданских свобод, запросили дополнительную информацию у нескольких из этих округов. Активисты интересуются подробной информацией о том, у кого есть доступ к журналам системы FRT (частные лица, местные власти, власти штата или федеральные власти) и будут ли изображения использоваться для совершения других действий (например, контроля за иммиграцией).

Данные об эффективности технологий распознавания лиц в условиях школы весьма скудные. Администраторы ценят преимущество активного видеонаблюдения за то, что оно позволяет автоматизировать процесс, для выполнения которого в противном случае потребовались бы значительные ресурсы. Тем не менее некоторые специалисты отмечают, что инциденты с применением насилия в школах, как правило, совершаются учащимися, которые имеют право находиться на территории кампуса, и, следовательно, система FRT, предназначенная для выявления тех людей, которым не разрешено входить на территорию школы, не играет большой роли при защите этих сообществ.

Правоохранительные органы

Правоохранительные органы на всех уровнях власти приняли систему FRT для достижения двух целей – проверки (подтверждения) личности или идентификации (распознавания) неизвестного лица. На местном уровне и уровне штата правоохранительные органы обладают определенной автономией в определении своей политики конфиденциальности данных.

Центр по вопросам личной информации и технологий при Правовом центре Джорджтаунского университета провел исследование «Perpetual Line-Up», посвященное использованию технологий распознавания

лиц 50 крупнейшими правоохранительными учреждениями страны. На рис. 2 представлены результаты, отражающие множество аспектов. Высокие оценки точности указывают на то, что агентства выполнили большую часть следующей работы: протестировали свои алгоритмы с Национальным институтом стандартов и технологий, заключили контракты с поставщиками, в которых оговаривается, что тесты на точность будут проведены, привлекли людей к проверке результатов запросов и использовали результаты FRT «только для ведения следствия». Агентства, выполнившие немногим меньше из вышеперечисленных действий, отнесены к категории «средняя точность», в то время как агентства, которые выполнили меньше всего работы, находятся в категории «низкая точность».

Что касается согласия на размещение в этих наборах данных, то организации с высокими оценками включают фотографии только арестованных лиц и исключают изображения из дел, по которым был вынесен оправдательный приговор или не было предъявлено никаких обвинений. Департаменты среднего звена использовали фотографии арестованных лиц, но удаляли их только после того, как человек подавал заявление с просьбой удалить его фото и получил на то разрешение. Подразделения с низким рейтингом включают в свои базы данных все снимки и фотографии, взятые из водительских удостоверений. Департаменты, занимающие верхние строчки в списке организаций, чья деятельность оценивается как удовлетворяющая требованиям прозрачности, позволяют законодательным органам или группам по защите гражданских свобод проводить проверку политики внедрения системы FRT. Департаменты, чья деятельность не является полностью прозрачной, не допустили заинтересованные группы к ознакомлению с политикой внедрения систем FRT, или же эта политика не была этими группами одобрена. У департаментов, оказавшихся в нижних строках списка по уровню прозрачности, отсутствует политика использования технологий распознавания лиц, с которой можно было бы ознакомиться.

На федеральном уровне сбор личной информации регулируется двумя законами: Законом о конфиденциальности 1974 г. и Законом об электронном правительстве 2002 г. Они предписывают правительственным программам уведомлять общественность о сборе, раскрытии и использовании личной информации через систему уведомления о регистрации и оценки последствий с точки зрения сохранения конфиденциальности

(Privacy impact assessment – PIA). ФБР имеет две базы данных, которые применяют систему FRT. Первая – база данных, в которой хранятся более 30 млн изображений лиц, соответствующих примерно 16,9 млн человек. Эта база данных межрегиональной фотосистемы, получившая название «Идентификация следующего поколения»⁶, состоит как из фотографий, сделанных криминальной полицией, так и гражданских фотографий, полученных из различных источников. Федеральное агентство или агентство штата может отправить изображение лица в ФБР, которое затем пришлет 50 наиболее точных совпадений, а также отпечатки пальцев и другую идентифицирующую информацию.

Указанная система FRT представляет собой схему идентификации «один – много»: одно изображение, представленное государственным агентством, сравнивается с 30 млн изображений и возвращается уже набор наиболее подходящих изображений. Изображения в базе данных могли быть собраны совместными усилиями, например фотография с водительского удостоверения будет представлять человека, который сидит перед камерой и (вероятно) соблюдает требования фотографа (он не пройдет мимо камеры или не попытается намеренно скрыть изображение). Однако ФБР хранит все изображения и делает их доступными для вспомогательного использования. Человек, фотографирующийся для получения водительского удостоверения, будет считать, что его изображение послужит для его идентификации представителями государственных или правоохранительными органами (например, когда его останавливают на трассе). Однако этот человек может не знать, что его изображения добавлены в базу снимков, которые будут проверены правоохранительными органами в соответствии с уведомлением о системе учета или PIA, опубликованным соответствующим государственным учреждением.

PIA для базы данных «Идентификация следующего поколения» детализирует ключевую информацию о конфиденциальности, точности и согласии субъектов, изображения которых включены в базу данных. Доступ к изображениям предоставляется только авторизованным пользователям правоохранительных органов, чьи личности и результаты поиска сохраняются в истории пользования системой. Результаты могут использоваться только для помощи в расследовании, но не для точной

⁶ Next Generation Identification (NGI) Interstate Photo System (IPS).

идентификации. В соответствии со стандартами Национального управления архивов и документации фотография может быть уничтожена либо по достижении субъектом возраста 110 лет, либо через семь лет после того, как администрация получит уведомление о его смерти. Что касается согласия, то любой человек, у которого запрашивают фотографию для оформления лицензии или найма на работу, вправе отказаться ее предоставить, но это может повлиять на исход дела, которое ведет заинтересованное агентство. Человек, чья фотография попала в базу данных в результате ареста, не может отказаться от внесения в эту базу данных. Наконец, оценивая точность, ФБР определило, что в 85% случаев при обнаружении не менее 50 результатов среди них будет фигурировать как минимум одно изображение интересующего объекта.

Вторая база данных ФБР – это Служба анализа, сравнения и оценки лиц (Facial Analysis, Comparison, and Evaluation – FACE), ее использование ограничивается собственными расследованиями бюро. Основное различие между двумя базами данных заключается в том, что FACE имеет доступ к фотографиям преступников из базы данных правоохранительных органов и изображениям, полученным от таких внешних партнеров, как Министерство обороны США, консульской базы данных Государственного департамента США, а также фотографиям преступников и людей, таковыми не являющихся, из 16 штатов – всего более 411 млн изображений. Обе базы данных имеют аналогичные стандарты конфиденциальности.

Во всех правительственных организациях закупка технологий распознавания лиц зависит от программного и аппаратного обеспечения, предоставляемого частным сектором. Недавно несколько компаний публично признали озабоченность по поводу воздействия этой технологии на гражданские свободы. Некоторые решили выступить за усиление защиты конфиденциальности на национальном уровне, в то время как другие решили не предлагать свои разработки правоохранительным органам. Угроза гражданским правам побудила политиков в Сан-Франциско и Массачусетсе объявить мораторий на системы FRT во всех правительственных учреждениях, находящихся в их ведении.

Частный сектор

Компании, осуществляющие свою деятельность во многих секторах

экономики, используют технологии распознавания лиц для предоставления инновационных услуг потребителям и организациям. Технологические компании выпустили на рынок такие устройства, как Apple iPhone X, которые применяют распознавание лиц для процессов аутентификации (по схеме «один – один»). Google и Facebook анализируют загруженные изображения, пытаясь сопоставить объекты со своими базами данных изображений от более чем 2 млрд активных пользователей (по схеме «один – много»). Другие коммерческие разработки в сфере FRT были проданы в качестве инструментов наблюдения государственным учреждениям, например Amazon Rekognition и Panasonic FacePRO. В частности, правоохранительные органы подверглись критике со стороны гражданских правозащитных групп за использование Rekognition. Однако применение технологий распознавания лиц частным сектором в США не регулируется единым сводом правил. Вместо этого на разных административных уровнях установлены руководящие принципы получения, анализа и коммерциализации изображений лиц.

На федеральном уровне биометрическая информация защищена в соответствии с законодательством, распространяемым по отдельным секторам и демографическим группам (табл. 3). Например, изображение лица ребенка в соответствии с Законом о защите личной информации о детях в Интернете от 1998 г.⁷ или идентифицируемое изображение в электронной медицинской карте в соответствии с Законом об ответственности и переносе данных о страховании здоровья граждан 1996 г.⁸ считается защищенной личной информацией. Приложения FRT, выходящие за рамки законов, указанных в табл. 3, не защищены федеральным законом.

В Иллинойсе, Вашингтоне и Техасе на уровне штата приняли законы, которые нацелены на использование частным сектором биометрической информации, такой как изображения лиц. В штате Калифорния также был принят аналогичный закон, который вступил в силу в 2020 г. Общей канвой этих законодательных документов является определение биометрических идентификаторов, которые включают в себя изображения лиц, описывая их как «геометрию лица» или уникальные биологические образцы, иден-

⁷ The Children's Online Privacy Protection Act of 1998 (Pub. L. 105-277, Title XIII).

⁸ The Health Insurance Portability and Accountability Act of 1996 (HIPAA).

тифицирующие человека. Важно, что компании вменяется в обязанность уведомить и получить согласие на любое коммерческое использование идентифицирующего изображения. Наконец, компании должны проявлять разумную осторожность в отношении доступа третьих лиц к этим данным и устанавливать ограниченные сроки хранения.

Одно из основных различий между законами этих штатов заключается в субъекте, уполномоченном обеспечивать их соблюдение. В Техасе и Вашингтоне эту роль выполняет только генеральный прокурор штата. В Калифорнии генеральный прокурор штата и потребитель разделяют ответственность за принятие мер против организаций, нарушающих меры защиты конфиденциальности. В Иллинойсе любое лицо имеет право возбудить дело против компании и получить компенсацию в размере от 1000 до 5000 долл. за каждое нарушение. В результате к таким компаниям, как Google, Facebook и Shutterfly, был предъявлен иск за сбор и маркировку информации о лицах пользователей. По судебным делам в Иллинойсе вынесли спорные решения. Некоторые иски были отклонены, поскольку компании утверждали, что хотя они и собрали биометрическую информацию, истцы не смогли доказать, какие «конкретные телесные повреждения» из-за действий ответчиков им были нанесены. Однако верховный суд Иллинойса недавно постановил, что нарушение закона было «реальным и значительным» ущербом, и, следовательно, дверь для дальнейших судебных исков открыта.

Помимо правительства в обсуждении защиты биометрической информации и ее последствий для частных компаний участвовали представители некоммерческого сектора. Один из наиболее важных форумов для этой дискуссии был организован Национальным управлением электросвязи и информации, входящим в состав Министерства торговли США. Управление организовало форум для некоммерческих организаций, целью которого являлось достижение консенсуса в отношении передовых методов распознавания лиц в коммерческих организациях. В форуме приняли участие две группы неправительственных организаций. Первая группа состояла из ассоциаций компаний частного сектора, которые представляют взгляды и интересы акционеров этих компаний перед государственными органами и общественностью. Во вторую группу вошли организации, отстаивающие права потребителей и общественные интересы.

Обе группы согласились с важностью пропаганды проблемы защиты потребителей на основе принципов справедливого использования информации, которые отражают международные стандарты защиты личной информации и были закреплены федеральным правительством в Законе о конфиденциальности 1974 г.⁹ Они включают в себя конкретные положения в отношении согласия, сохранения информации и доступа к данным. Однако главным предметом разногласий при обсуждении принципов справедливого использования информации являлся вопрос добровольности или обязательности этих принципов. Группа представителей компаний выступала за введение добровольных стандартов, в соответствии с которыми каждая компания решала бы, как защитить свои данные системы FRT, в то время как группа представителей потребителей выступала за обязательное соблюдение принципов, реализуемых через законодательство, для защиты потребителей. Это разногласие привело к тому, что несколько групп по защите прав потребителей покинули форум.

Национальная безопасность

Министерство обороны и Министерство национальной безопасности США разработали автоматизированные системы биометрической идентификации для выдачи документов лицам, не являющимся гражданами США, подозреваемым в терроризме или представляющим угрозу безопасности войсковых подразделений. Как только информация (например, фотография) о подозреваемом получена, эти агентства вводят ее в систему идентификации, которой могут пользоваться и другие федеральные ведомства по схеме «один – много». Из-за своего статуса подозреваемые не могут отказаться от включения их биометрической информации в систему, но им дается возможность исправить данные об их классификации.

В Соединенных Штатах внедрение системы FRT было обусловлено в первую очередь иммиграционным процессом. Госдепартамент США использует систему, работающую по схеме «один – много», способную идентифицировать человека, который может представлять угрозу безопасности, в процессе подачи заявления на визу. Система сравнивает фотографии заявителей с фотографиями в базах данных, где хранятся изображения людей, находящихся в списке Национального контртеррористического центра, которым было отказано в выдаче визы. Для этой программы заявители предоставляют свои данные добровольно, потому

⁹ The Privacy Act of 1974 (Pub. L. 93-579).

что они пытаются получить разрешение на въезд в страну, а Соединенные Штаты уведомляют их о том, что информация о них может быть сохранена для перекрестной проверки личности.

Министерство национальной безопасности все чаще использует технологии распознавания личности в своей работе в аэропортах. Проект Министерства по сопоставлению лиц – это система, работающая по схеме «один – один», которая проверяет личность путешественника путем сравнения его лица с лицом на фотографии. Для этого специальный прибор сканирует электронный паспорт с микрочипом и делает снимок лица путешественника, для чего его могут попросить снять головной убор или очки. Затем система использует технологию распознавания лица для сравнения снимка путешественника с данными его электронного паспорта. Эта система имеет несколько характеристик. Во-первых, FRT используется для определения наличия совпадения проверенной фотографии в паспорте с фотографией, сделанной в аэропорту. Во-вторых, предполагается, что для обоих снимков (снимка для паспорта и снимка в аэропорту) человек знал, что его фотографируют, и выполнял любую просьбу, связанную с улучшением качества снимка. Хотя путешественникам не разрешается отказываться от этой процедуры, они могут получить компенсацию в рамках программы Министерства национальной безопасности США «Traveler Redress Inquiry Program», и в системе сохраняются изображения только тех лиц, которые подлежат вторичной проверке. В 2017 г. Министерство внесло предложение о создании технологии для идентификации людей, въезжающих в страну через сухопутные границы, которые позволили бы субъектам оставаться в своих автомобилях (по схеме «один – много»).

Помимо пограничного контроля Министерство национальной безопасности изучает возможность проверки иммигрантов с помощью социальных сетей, но здесь пока еще много проблем – технических, организационных, измерительных и юридических, – которые необходимо решить до внедрения системы. В министерстве и в его оперативных подразделениях (например, таможенной и пограничной службах США) начали использовать социальные сети на постоянной основе для выполнения ключевой задачи: проверки людей, желающих въехать в Соединенные Штаты. Часть аналитических возможностей включает распознавание лиц, которое важно для определения личности, т. е. сбора информации, которую сам субъект дает

о себе. Министерство национальной безопасности считает, что социальные сети открывают ряд дополнительных возможностей, и приступило к изучению различных технических подходов для наиболее эффективного использования информации, размещенной в этих сетях.

3. Технологии распознавания лиц на практике

Рассмотрим два варианта использования технологий распознавания лиц для целей безопасности (см. табл. 1): первый – проверка подлинности паспорта на пограничном контроле и второй – наблюдение за лицом в толпе в аэропорту. Если первый вариант связан с низким риском конфиденциальности и высокой точностью, то второй – с высоким риском конфиденциальности и низкой точностью. Эти варианты использования намеренно носят общий характер, чтобы проиллюстрировать проблемы конфиденциальности и предвзятости, а также действия, которые могут быть предприняты для устранения недостатков. Следует отметить, что Департамент национальной безопасности США активно работает над решением этих проблем, например путем внедрения принципов справедливого использования информации (например, транспарентности, ограниченного времени хранения данных) в демонстрационные технологии своих пограничных контрольно-пропускных пунктов.

Проверка подлинности паспорта на пограничном контроле

Этот вариант использования технологий распознавания лиц соответствует общему сценарию паспортного контроля в аэропорту, цель которого – подтвердить, что лицо путешественника соответствует фотографии в паспорте. Путешественник в пункте пограничного контроля обычно предъявляет паспорт или другой документ, в котором есть фотография, подтверждающая его личность. Некоторые международные аэропорты внедрили систему FRT для сравнения информации из электронного паспорта, который сканируется, с фотографией владельца паспорта, сделанной на пункте пограничного контроля. Обычно это сравнение происходит во время первичной проверки. После этого сотрудник службы пограничного контроля может направить путешественника на вторичный досмотр, если он решит, что между фотографиями нет соответствия (согласно данным FRT) или если путешественник может представлять потенциальную опасность. При вторичной проверке фотография, сделанная в аэропорту, может пройти более строгую проверку или ее отправят на хранение.

Рассматриваемый вариант использования технологий распознавания лиц помимо подтверждения личности может включать в себя также другую функцию – сопоставления информации о путешественнике с черным списком (например, списком наблюдения за террористами) людей, которым не разрешен въезд на территорию страны или которые подлежат дальнейшему допросу. Такая процедура изменяет потенциальную архитектуру хранения данных и вводит дополнительные соображения в вопросе конфиденциальности, точности и возмещения ущерба. Например, сопоставление с черным списком увеличивает объем необходимой информации и вторичное использование данных, что может потребовать безопасного подключения к конфиденциальным базам данных. В целом этот пример использования наглядно показывает, как дополнительные функции системы делают ее более сложной и уязвимой.

Проверка подлинности паспорта на пограничном контроле менее других нарушает конфиденциальность, так как люди осведомлены, когда и где следует предоставлять личные данные. Таким образом, у них есть некоторая степень контроля над тем, как используются их данные. Однако риски, связанные с ошибкой сопоставления FRT или вторжением в частную жизнь, могут нанести ущерб, в том числе в результате ареста, физического досмотра или задержки во время поездки.

Функции применения системы могут включать в себя систему разделения набора данных, которая позволяет хранить полученные данные в разных местах. Черный список должен храниться в базе данных и на сервере, отличном от предназначенных для хранения паспортных данных. Разделение баз данных не обеспечивает надежную защиту от хакеров, которые могут получить доступ к обеим базам и связать информацию между собой, но тогда им придется потратить значительно больше времени и сил, чтобы получить незаконный доступ к такой информации, поскольку необходимо взломать большее число серверов и учетных данных. Записи транзакций или журналы событий также должны храниться в отдельных базах данных с контролем доступа, отличных от тех, где хранится личная паспортная информация. Это ограничит доступ уполномоченного персонала и создаст дополнительное препятствие для злоумышленников, которые хотят получить доступ ко всем базам данных и связать между собой оба набора информации. Целостность данных изображения важна для точной и надежной обработки, а также для обеспечения качества сделанного изображения путешественника. Власти

должны контролировать места, где производится съемка изображений, чтобы не допустить физических взломов.

Минимизация данных часто относится к уменьшению необходимости поддерживать данные, связывать их с другими данными или получать доступ к личной информации. Однако в этом случае система FRT была специально разработана для увязки личной информации с определенным лицом. Возможности минимизации данных включают хранение только определенных элементов паспортных данных и ограничение доступа к ним. В этом случае системе в аэропорту доступна только паспортная информация, которая необходима для выявления совпадения (например, номер паспорта, извлеченные изображения элементов лица и, возможно, имя путешественника). Для сопоставления лица с данными черного списка может потребоваться дополнительная информация. Методы минимизации данных могут включать в себя передачу и сохранение только извлеченных и хешированных характеристик после обработки изображения, в отличие от передачи и сохранения полного изображения. Один из вариантов – сделать это локально на оборудовании, снимающем изображение. Обратная сторона медали такой системы заключается в том, что отсутствует возможность проверить информацию или повторно протестировать совпадение лиц.

В этом случае путешественник является активным участником процесса распознавания лиц по всем компонентам изображения. Пассажир, вероятно, знает, что сканирование его паспорта и фотографирование означает, что два изображения будут сравниваться и таким образом его личность будет проверена. Подробное описание политики конфиденциальности во время досмотра может быть излишним, но предоставить некоторую информацию о защите данных будет уместно, особенно если у путешественника есть альтернатива. Однако малоопытный или наивный путешественник может не знать о компоненте черного списка системы. Сравнение его данных с данными черного списка будет считаться вторичным использованием данных, что может рассматриваться как вторжение в частную жизнь. Представьте, что невиновный путешественник добросовестно вводит собственный паспорт, но система выдает ложный результат. Такая ошибка может нанести реальный вред, если его физически задерживают, обыскивают или конфискуют его вещи. Уведомление об использовании данных особенно важно для возмещения ущерба, так как

путешественники не могут исправить ошибки, если у них нет информации о системе, которая их порождает.

Путешественники, которые понимают, на каком этапе проверки возникла ошибка, могли бы лучше сотрудничать и предоставить дополнительные материалы. Общая проблема прозрачности системы заключается в том, что злоумышленники могут использовать любые знания, полученные о системе, для игры в нее. Например, если снятие очков успешно решает проблему неудачного совпадения, это может означать, что ношение очков может быть эффективным взломом для автоматических киосков, хотя и не в присутствии сотрудника пограничного контроля (например, когда путешественников направляют на вторичный досмотр). В этом случае неясно, усугубляется ли какой-либо из возможных взломов этой системы уведомлением: в отдельных случаях злоумышленники, например, могут предположить, что компонент черного списка существует, или могут знать, что они находятся в черном списке.

Путешествуя самолетом, человек, разыскиваемый за совершение преступления, возможно попытается присвоить себе имя, которое не вызовет подозрений властей. Для этого он может прибегнуть к взлому, который, по его мнению, с наибольшей вероятностью позволит обойти системы безопасности. В ответ власти, вероятно, будут модернизировать свои системы, например, посредством ввода более строгих протоколов безопасности, которые могут повлиять на время, затрачиваемое невиновным человеком на подтверждение своей личности. Поскольку большинство пунктов пограничного контроля обслуживаются людьми, преступники вряд ли «подделают» другую личность, используя фотографии, видео или трехмерные маски во время фотосъемки. Однако в некоторых странах устанавливаются системы, которые передают задачи проверки личности автоматизированным службам. В этих случаях потенциальные злоумышленники могут не только избежать контакта с человеком, но и получить больше свободы, выдавая себя за другую личность с помощью фотографий или видео. Преступники могут попытаться избежать сопоставления с данными из черного списка, прибегнув к морфингу. Другими словами, изображение, использованное преступником в проездном документе, может быть совмещено с изображением похожего на него человека. Преимущество этого метода заключается в том, что характеристики лица

могут выглядеть достаточно похожими, на взгляд сотрудника пограничного контроля, и обходить системы предупреждения из черного списка FRT.

В процессе проверки паспорта возможна определенная предвзятость. Путешественник на контрольно-пропускном пункте позирует фотографу, затем полученная фотография сравнивается с фотографией в паспорте (по схеме «один – один») и, возможно, со списком преступников или террористов, т. е. базой данных изображений лиц (по схеме «один – много»).

Когда FRT применяются для сопоставления фотографии контрольно-пропускного пункта с фотографией в паспорте, риск предвзятости лежит в двух плоскостях. Во-первых, обучающие данные, использованные для построения алгоритма FRT, могли недостаточно представить или избыточно представить определенные группы людей. Это приведет к неравным шансам на то, что FRT выдаст истинный результат положительного совпадения, тем самым увеличивая вероятность отказа во въезде в страну определенным группам путешественников.

Следующая возможность предвзятости на контрольно-пропускном пункте и в совпадении паспортов заключается в интерпретации результатов человеком. В зависимости от того, как представлены результаты (например, простая оценка соответствует / не соответствует), сотруднику паспортного контроля требуется принять окончательное решение о том, следовать ли рекомендации алгоритма и разрешить въезд в страну. Уверенность сотрудника в принятом решении, основанном на рекомендации алгоритма, может зависеть от субъективного суждения о том, совпадают ли фотографии, а также от явного или неявного предубеждения в отношении определенных групп людей.

Сравнение фотографий, сделанных на контрольно-пропускном пункте, с фотографиями из базы данных с изображениями лиц может внести дополнительный риск систематической ошибки в целевой набор данных. Некоторые люди, относящиеся к группам, находящимся под наблюдением, например расовые меньшинства, представителей которых арестовывают с непропорционально высокой частотой, чрезмерно представлены в базе данных по лицам.

Такие группы с большей вероятностью будут демонстрировать положительные черты лица, что выделяет их как путешественников с высоким риском и увеличивает вероятность отказа во въезде в страну. Даже если система FRT имеет высококачественные обучающие данные и была тщательно протестирована на предмет предвзятости и справедливости, простое существование контрольно-пропускного пункта может оказать сдерживающее влияние на въезжающих. Меньшинства или исторически преследуемые группы реже доверяют государственным технологиям, а наличие контрольно-пропускного пункта, где нужно представиться и дать согласие на идентификацию по фотографии и сопоставление лиц, может выступать сдерживающим фактором для людей, желающих путешествовать. Следовательно, прозрачность и уведомление о системах FRT, возможно, потребуют особой осторожности, чтобы смягчить эти опасения.

Резюмируя, можно сказать, что в обществе отмечается беспокойство относительно вопросов конфиденциальности и справедливости при применении технологий распознавания лиц.

- Добавление вторичного использования изображений помимо проверки паспорта увеличивает сложность системы. Возрастает нагрузка, связанная с защитой данных, что затрудняет процесс минимизации данных.

- Отсутствует возможность простого исправления ошибок после их возникновения. Если лицо, чье изображение сопоставляется, не может легко исправить ошибки или потребовать внести исправления, то система воспринимается как несправедливая, и люди не смогут защитить конфиденциальность данных.

- Обучающие данные являются возможным источником систематической ошибки. Информация об определенной категории путешественников может не фигурировать в обучающих данных и, следовательно, порождает предвзятость.

- Когда результаты FRT не проверяются людьми, возможны взломы системы и обман с использованием фотографий, видео или физических масок.

- Когда не делается фотография головы человека, то при попытках взломать систему распознавания злоумышленники могут использовать морфинг.

Наблюдение за лицом в толпе в аэропорту

Через панамский аэропорт Токумен ежедневно проходит около

41 тыс. человек. Когда они попадают в поле зрения одной из 149 расположенных в аэропорту камер, способных фиксировать черты лица, без ведома большинства путешественников их изображение сравнивается с изображениями в базе данных, содержащей информацию о людях, находящихся в национальном и международном розыске. Это пример механизма идентификации по схеме «много – много», при котором лица в толпе сопоставляются с лицами из базы данных. Кроме того, путешественнику не предоставляется возможность дать согласие на использование своего изображения для анализа. Система Tocumen FRT (FaceFirst Guardian – коммерческая разработка) заявляет о возможности обнаруживать до 30 подозреваемых каждый день. Это означает, что по крайней мере 30 из 41 000 пассажиров ежедневно отмечаются как подозреваемые. Следовательно, система FRT должна демонстрировать чрезвычайно высокую степень достоверности и точности, поскольку 99% выборки будет предлагать более 400 (!) ложноположительных результатов каждый день.

Некоторые аспекты использования FaceFirst Guardian в аэропорту Токумен было бы актуально рассмотреть для других аэропортов. Во-первых, основные компоненты системы FRT обрабатываются запатентованной коммерческой технологией. Это актуально для вопроса безопасности, в том числе для вопроса о месте хранения информации и о том, какая информация будет дублироваться. Во-вторых, люди несут ответственность за действия в соответствии с результатами FRT. После того как совпадение обнаружено, агентам в аэропорту отправляется предупреждение, которое, вероятно, включает совпадающие фотографии, местоположение человека и, возможно, другую идентифицирующую информацию. На этом этапе агент будет полагаться на способность распознавать человеческое лицо, чтобы идентифицировать подозреваемого в переполненном аэропорту. В-третьих, камеры, которые собирают изображения толпы, размещаются в узких местах, например на эскалаторах. Вероятно, это связано с тем, что во время съемки путешественники будут двигаться медленнее, что обеспечит лучшее качество изображения. Кроме того, если совпадение обнаружено, подозреваемый, скорее всего, будет зажат в толпе или станет двигаться медленно, что даст агентам больше времени для реагирования, прежде чем подозреваемый направится в другую часть аэропорта.

По сравнению с первым вариантом использования технологий распознавания лиц этот вариант нарушает конфиденциальность, поскольку не дает пользователю никакой возможности контролировать, как используются данные о нем. Более того, риски таких вторжений могут быть опасными, включая аресты, физические обыски или отложенные поездки. В этом сценарии технологии с усовершенствованной защитой предлагают некоторые возможности для защиты конфиденциальности.

Скорее всего, технологии распознавания лиц в аэропорту сопоставляют людей, снятых через камеры наблюдения, с изображениями и информацией о подозреваемых в централизованной базе данных, полученной от национальных и международных правоохранительных органов. Учитывая конфиденциальный характер этой базы данных, она может быть подвержена серьезным постоянным угрозам, особенно если преступные организации или другие субъекты хотят изменить или модифицировать данные (т. е. удалить или заменить изображения). Следовательно, требуется высокий уровень безопасности как для данных, хранящихся в этой базе данных, так и для данных, вводимых в систему. Чтобы исправить свою работу, система должна будет вести журналы транзакций и решений. Их следует тщательно защищать и, по возможности, очищать от личной информации.

Рекомендуется удалять в режиме реального времени фотографию, не имеющую совпадений. База данных, содержащая изображения путешественников, включает конфиденциальную информацию, которая может подвергнуться риску со стороны желающих атаковать систему аэропорта злоумышленников. Кроме того, путешественники могут пожелать защитить свою информацию о поездках от конкурентов, преследователей и т. д., поэтому было бы разумно хранить изображения путешественников только в течение короткого периода времени. Фотография, которая совпадает с изображением подозреваемого, скорее всего, должна храниться дольше, чтобы сотрудники правоохранительных органов могли отреагировать и просмотреть ее. В предыдущем примере использования мы обсуждали возможность хранения и совместного использования только извлеченных черт лица вместо полного изображения. В этом случае мы отмечаем, что если правоохранительные органы или службы безопасности должны обыскать аэропорт в поисках подозреваемого на основе изображения, то сохраняется и анализируется полное изображение. Это означает,

что цели системы исключают по крайней мере один вариант повышения конфиденциальности.

Сама природа этой системы предполагает относительно мало возможностей для уведомления. Фотографии собираются без сотрудничества с испытуемыми. Это связано с тем, что разработчики систем слежения в аэропорту могут скрыть камеры, если сочтут, что гораздо важнее обнаружить подозреваемого, чем осведомить путешественников о присутствии камер. Изображения подозреваемых могли быть получены, если кто-то находился под арестом, но изображения могли быть также собраны через социальные сети или камеры наблюдения. Вопросы доступа и возмещения ущерба особенно усложняются в случае ложных срабатываний. Невинные путешественники могут не знать, включены ли их фотографии в базу данных подозреваемых. Как только они узнают об этом, у них должна быть возможность оспорить решение внести их базу данных. Кроме того, как отмечалось выше, существует чрезвычайно низкая базовая частотность истинных результатов, и каждый день могут выдаваться сотни ложноположительных ответов. Если FRT сравнивает путешественника с подозреваемым, система возмещения ущерба (например, показ агенту документов, удостоверяющих личность) должна быть доступной и эффективной.

Чтобы избежать обнаружения камерами, включенными в систему распознавания лиц, люди могут выбрать методы временной или постоянной маскировки. Такие методы могут быть подходящими для публичных, неконтролируемых пространств, где от субъектов не требуется согласие на позирирование для фотографий. Временная маскировка – шляпы, очки, искусственные волосы на лице или макияж – относится к категории гибких, поскольку элементы взаимозаменяемы и легко применяются перед объективом камеры. Та маскировка, которая может покрывать большую площадь лица, оставляет меньше информации, связывающей личность с фотографией. Под постоянным методом маскировки понимается, например, хирургическая операция на лице. Его преимущество в том, что оно делает ненужными искусственные барьеры. Однако если новые черты лица человека обнаруживаются и каталогизируются FRT, то может потребоваться дальнейшая операция или временная маскировка, чтобы избежать обнаружения.

Общее наблюдение в аэропорту за «лицами в толпе» сводится к проведению многочисленных несогласованных сравнений по схеме «много – много». Более того, процесс в значительной степени зависит от участия человека, поскольку ожидается, что агенты будут использовать результаты FRT для идентификации реальных людей и взаимодействия с ними, как это происходит в аэропорту Панама. Этот крупномасштабный многофазный процесс допускает несколько форм потенциальной систематической ошибки. В данном случае опасения по поводу предвзятости связаны в основном с ложноположительными результатами. Ложные результаты могут возникать из-за предвзятости, содержащейся либо в данных обучения алгоритма, либо в целевых данных, с которыми сопоставляются лица, выхваченные из толпы. Примером тому может быть непропорциональное присутствие меньшинств в базах данных правоохранительных органов (например, фотографии из протоколов задержания), о которых упоминалось ранее. Следует отметить, что это исследование в основном относится к базам данных США, результаты в других странах могут отличаться.

Отсутствие согласия на сопоставление фотографий является еще одним источником потенциальной предвзятости. В ситуациях с неидеальными фотографиями (например, закрытое лицо, различия в освещении и ракурсе) алгоритмам необходимо стандартизировать фотографии, что требует дополнительных функций программы, в которых предвзятые данные обучения могли бы играть не последнюю роль. Учитывая, что агентам поручено сопоставить фотографии лиц с людьми, находящимися в определенном месте (т. е. ограниченное сопоставление по схеме «один – много»), участие человека может привести к предвзятым конечным результатам всего процесса FRT. Как отмечалось ранее, люди-наблюдатели проявляют множество предубеждений, (например, лучше умеют сопоставлять лица своей расы), а также имеют множество явных и неявных стереотипов по расе, полу, религии или сексуальной ориентации. Любое из этих предубеждений может создать значительные неудобства путешественникам. Масштабность наблюдения в аэропорту усиливает потенциальное влияние предвзятости. Сопоставления по схеме «много – много» имеют более высокий процент ошибок, чем по схеме «один – один» или «один – много». Тем не менее даже если бы уровень ошибок был небольшим, абсолютное число неправильно идентифицированных людей, которые затем были задержаны и допроше-

ны, может представлять значительный общий ущерб для путешествующего населения. Наконец, как и в случае с отдельными контрольно-пропускными пунктами, наличие массового наблюдения может удерживать путешествующих от совершения обычных действий в общественных местах (например, есть, делать покупки в окрестностях аэропорта).

Таким образом, имеется несколько потенциальных проблем, указывающих на озабоченность по поводу конфиденциальности и справедливости.

- Хотя согласие и контроль являются необходимыми составляющими защиты конфиденциальности, система практически не предлагает возможности для уведомления или выбора.

- Если человек, чье изображение сравнивается, не может исправить или требовать исправления в случае возникновения ошибок, система будет считаться несправедливой, и люди не смогут защитить свою конфиденциальность.

- Обучающие данные являются возможным источником систематической ошибки. Обучающая информация может не отражать данные о всех группах путешественников, и здесь может крыться предвзятость.

- Базовый показатель потенциальных совпадений крайне низок. Обработка большого числа ложных результатов может дорого обойтись и вызвать недоверие к системе.

- Интерпретация результатов человеком вносит еще больше предубеждений и требует дополнительного хранения изображений или видео лиц, снятых анфас.

- Временные средства маскировки личности (шляпы, очки, макияж) хорошо подходят для больших, многолюдных мест, таких как аэропорты.

Приложение

Рисунок 1. **Схема компромисса между точностью и конфиденциальностью в технологии распознавания лиц**

Рисунок 2. **Отдельные результаты исследования «Perpetual Line-Up»**

Таблица 1. Примеры использования технологий распознавания лиц по степени согласия и схеме распознавания

Тип согласия	Схема распознавания	
	Проверка подлинности лица («один – один»)	Идентификация («некоторые – много»)
Субъект согласен	<ul style="list-style-type: none"> • Проверка подлинности паспорта на таможенном контроле • Аутентификация устройства 	<ul style="list-style-type: none"> • Разрешение идентификации личности в социальных сетях • Визовый контроль
Субъект не согласен	<ul style="list-style-type: none"> • Фотографии, сделанные правоохранительными органами • Проверка личности задержанного 	<ul style="list-style-type: none"> • Наблюдение за лицом в толпе в аэропорту • Наблюдение на улицах • Наблюдение в школах

Таблица 2. Некоторые направления политики регулирования программы технологий распознавания лиц по секторам и административным уровням

Сектор	Административный уровень		
	Местный уровень	Уровень штата	Федеральный уровень
Школы	х	х	
Правоохранительные органы	х	х	х
Частный сектор		х	х
Национальная безопасность			х

Таблица 3. Примеры федеральных законов, регулирующих сбор, использование и хранение личной информации

Сфера	Область действия
Здоровье	Закон «Об ответственности и переносе данных о страховании здоровья граждан» (HIPAA) регулирует раскрытие индивидуально идентифицируемой медицинской информации, которая собирается соответствующими медицинскими учреждениями, и устанавливает стандарты защиты данных
Дети	<p>Закон 1998 года «О защите личной информации о детях в Интернете» [The Children's Online Privacy Protection Act of 1998 (Pub. L. 105-277, Title XIII)] в целом запрещает сбор в Интернете личной информации от детей младше 13 лет без поддающегося проверке согласия родителей</p> <p>Закон «О семейных правах на образование и неприкосновенность частной жизни» [The Family Educational Rights and Privacy Act (Pub. L. 93-380, 1974, § 513, as amendments to the General Education Provisions Act)] регулирует раскрытие личной информации из документов об образовании</p>
Торговля	Федеральная торговая комиссия (FTC) отвечает за установление правил и преследование недобросовестной и вводящей в заблуждение торговой практики. Большая часть правоприменения, связанного с защитой частной информации, сводится к обеспечению соблюдения добровольной политики конфиденциальности, принятой компаниями
Кредит	Закон «О справедливой кредитной отчетности» [The Fair Credit Reporting Act (Pub. L. 91-508, 1970, Title VI, as amendments to the Consumer Credit Protection Act)] регулирует раскрытие личной информации, собранной или используемой для определения права на получение кредита, страхования или трудоустройства
Электронная коммуникация	<p>Закон «О конфиденциальности электронных сообщений» [The Electronic Communications Privacy Act (Pub. L. 99-508, 1986)] запрещает перехват и раскрытие электронных сообщений третьими сторонами, если не применяется указанное исключение</p> <p>Закон «О компьютерном мошенничестве и злоупотреблении» [The Computer Fraud and Abuse Act (Pub. L. 99-474, 1986)] запрещает получение информации с защищенного компьютера посредством преднамеренного доступа к нему без разрешения или с превышением разрешенного доступа</p>
Финансовые институты	Закон Грэмма – Лича – Блайли (The Gramm – Leach – Bliley Act [Pub. L. 106-102, 1999]) регулирует раскрытие закрытой информации, которую собирают финансовые учреждения, и устанавливает стандарты безопасности данных

Обзор выполнен на основе следующих публикаций:

1. Yeung, Douglas, Rebecca Balebako, Carlos Ignacio Gutierrez Gaviria, and Michael Chaykowsky (2020), *Face Recognition Technologies: Designing Systems that Protect Privacy and Prevent Bias*, Homeland Security Operational Analysis Center operated by the RAND Corporation, RR-4226-RC, 2020. – www.rand.org

Аэронавтика и космос

Биотехнологии и генетика. Сельское хозяйство, пищевая и химическая промышленность

**Информационные
и телекоммуникационные технологии
и вычислительная техника**

Исследования в области ядерной и квантовой физики

Медицинские технологии и оборудование

Нанотехнологии и новые материалы, микроэлектроника

Социальные и экономические науки и статистика

Энергетика и транспорт

Экология и рациональное природопользование