УДК 347.121.2 Правоведение. 2024. Т. 68, № 2

Правовая защита права гражданина на изображение лица при применении технологии распознавания лиц в законодательстве Китая*

Ш. Цзя, Ц. Чжан

Для цитирования: *Цзя Ш., Чжан Ц.* Правовая защита права гражданина на изображение лица при применении технологии распознавания лиц в законодательстве Китая // Правоведение. 2024. Т. 68, № 2. С. 271–283. https://doi.org/10.21638/spbu25.2024.210

В эпоху быстрого развития больших данных биометрическая технология распознавания лиц, идентифицирующая и подтверждающая личность человека по его лицу, постепенно становится объектом внимания общественности. В КНР данная технология стала незаменимым средством сбора информации для государственных и коммерческих организаций. Технология распознавания лиц может быть использована для быстрой идентификации личности и повышения эффективности и точности работы различных служб. Однако у медали две стороны. Широкое использование технологии распознавания лиц оказало влияние на традиционную систему защиты прав гражданина на изображение лица, поэтому соответствующие законы должны быть усовершенствованы в целях предотвращения утечек изображения лица и злоупотреблений использованием изображения лица. Только синхронное продвижение развития технологии распознавания лиц и совершенствование законодательства может обеспечить дальнейшую защиту права гражданина на изображение лица. В данной статье анализируется применение технологии распознавания лиц и связанные с этим риски, объясняется имеющаяся законодательная основа и ее недостатки в Китае, а также выдвигаются соответствующие предложения по дальнейшей защите собранной информации об изображении граждан в рамках технологии распознавания лиц.

Ключевые слова: технология распознавания лиц, защита изображения лица, чувствительные персональные данные, право КНР, искусственный интеллект, цифровизация, личные права, информация.

Введение

В XXI в. биометрическая аутентификация становится неотъемлемой частью повседневной жизни. Технология распознавания лиц создает набор данных о чертах лица, который затем сравнивается с изображением исследуемого лица, что позволяет достичь цели идентификации и подтверждения личности. В отличие от традиционных персональных данных, таких как ФИО, номер удостоверения личности, дата рождения, адрес, номер телефона и т. д., биометрические

Цзя Шаосюе — д-р юрид. наук, Шанхайский политико-юридический университет, Китай, 201701, Шанхай, пр. Вайцинсун, 7989; ys02302041@126.com

Чжан Цзинсинь — мл. науч. сотр., Шанхайский политико-юридический университет, Китай, 201701, Шанхай, пр. Вайцинсун, 7989; ys02302041@126.com

* Данная статья подготовлена в рамках общего проекта Национального фонда общественных наук КНР «Исследование механизма правового управления безопасностью данных в ШОС» (№ 22BFX160). 基金项目:国家社科基金一般项目“上合组织数据安全法律治理机制研究”（编号:22BFX160）研究成果。

персональные данные являются уникальными для идентификации личности[1]. В целом в приложениях распознавания лиц действует «живое» обнаружение идентифицируемого лица, т. е. идентифицируемое лицо должно выполнить комбинацию действий, например: моргание, открытие рта, кивок головой, чтобы его можно было опознать как реальное действующее лицо.

В Китае данные и информация, полученные с помощью технологии распознавания лиц, широко используются в качестве способа идентификации во многих областях, таких как транспорт (например, проверка безопасности в метро, продажа билетов на поезд и т. д.), контроль доступа в жилой комплекс, учет рабочего времени, онлайн-банкинг и мобильные платежи, поиск людей и потерянных вещей. Время вариации способов применения распознавания лиц быстро расширяются, масштаб мирового рынка достиг 2,391 млрд долл. США, что демонстрирует огромный потенциал. В настоящее время Китай занимает третье место в мире по количеству специалистов в вышеназванной области, а объем рынка составляет 440 млн долл. США[2].

Однако широкое использование технологии распознавания лиц создает новые проблемы для защиты персональных данных. Прежде всего наибольший правовой риск технологии распознавания лиц по сравнению с биометрическими технологиями заключается не в самой технологии, а в способности прямо или косвенно идентифицировать и сопоставить субъект информации через предварительно сохраненную биологическую информацию с помощью алгоритмов и анализа данных, что, в свою очередь, может в конечном итоге сформировать совокупность конфиденциальных и неконфиденциальных персональных данных. Другими словами, утечка информации о изображении лица не ограничивается информацией об изображении лица, за ней стоит целый ряд индивидуальной информации, включая семейное положение, активы, образование, занятость и т. д.[3]

Злоупотребление системой распознавания лиц может представлять угрозу безопасности личного имущества. Существует множество случаев утечки информации об изображении лица, что приводит к незаконной выдаче займов, мошенничеству, нарушению прав на частную жизнь и репутацию. Некоторые преступники используют незаконно полученные фотографии и другую личную информацию для создания 3D-изображений лица с целью кражи денег с чужих счетов Alipay[4]. С развитием технологий риск взлома систем распознавания лиц постепенно возрастает[5].

---

[1] 付微明. 个人生物识别信息的法律保护模式与中国选择 // 华东政法大学学报.2019.№ 6.页88 [*Фу Вэймин.* Модель правовой защиты личной биометрической информации и выбор Китая // Журнал Восточно-Китайского университета политических наук и права. 2019. № 6. С. 88].

[2] 蒋洁. 人脸识别技术应用的侵权风险与控制策略 // 图书与情报.2019.№ 5.页59 [*Цзян Цзе.* Риск нарушения прав и способы контроля при применении технологии распознавания лиц // Книга и сведения. 2019. № 5. С. 59].

[3] 胡凌. 刷脸：身份制度、个人信息与法律规制 // 法学家.2021.№ 2.页43–45 [*Ху Лин.* Скачивание лица: система идентификации, персональные данные и правовое регулирование // Юрист. 2021. № 2. С. 43–45].

[4] 详见浙江省衢州市中级人民法院（2019）浙08刑终333号刑事裁定书；四川省成都市郫都区人民法院（2019）川0124刑初610号 [Определение по уголовному делу № 333 «Чжэцзян 08-2019 г.» Народного суда средней ступени города Цюйчжоу, провинция Чжэцзян; Решение по уголовному делу № 610 «Сычуань 0124-2019 г.» Народного суда района Пиду, город Чэнду, провинция Сычуань].

[5] 苗杰. 人脸识别"易破解"面临的风险挑战及监管研究 // 信息安全研究. 2021.№ 10.页986 [*Мяо Цзе.* Исследование риска и контроля «легко взламываемой» технологии распознавания лиц // Исследование по безопасности информации. 2021. № 10. С. 986].

1. Правовая основа биометрической идентификации лица в Китае

В настоящее время китайский законодатель сильно обеспокоен влиянием искусственного интеллекта на существующие законы и стремится адаптировать законодательный массив к требованиям эпохи искусственного интеллекта. Правовое регулирование распознавания лиц в законодательстве Китая использует модель интеграции публичного и частного права, в рамках публичного права регулирует и контролирует деятельность по распознаванию информации о лицах, а в рамках частного права разъясняет права физических лиц на пользование личной информацией. В данной статье перечислены основные положения, которые могут помочь российским ученым понять основные соответствующие законодательные положения в Китае.

Закон КНР от 31.10.1993 г. № 11 «О защите прав потребителей»[6] впервые закрепил обязанности операторов по сбору и использованию персональных данных потребителей в ходе своей деятельности.

Закон КНР от 07.11.2016 г. № 53 «О сетевой безопасности»[7] включает персональные данные в качестве объекта защиты, устанавливает в ст. 40–50 принципы, которым необходимо следовать при сборе персональных данных, порядок сбора, хранения и использования персональных данных, а также подчеркивает право пользователя на распоряжение персональными данными и обязанности оператора сети.

Гражданский кодекс КНР от 28.05.2020 г.[8] (далее — ГК КНР) содержит положения о защите персональных данных в разделе «личные права» (ст. 1034–1039), включая биометрические данные как одни из персональных данных. Кроме того, в ГК КНР также уточнены принципы законности, необходимости и обоснованности, принципы информированного согласия и принципы ограничения передачи при обработке персональных данных, что создает механизм гражданской правовой защиты персональных данных.

В 2021 г. судебный комитет Верховного народного суда КНР опубликовал разъяснение «О некоторых вопросах применения законодательства при рассмотрении гражданских дел, связанных с использованием технологии распознавания лиц при обработке персональных данных» (далее — Разъяснение)[9]. Поскольку Разъяснение является специальным судебным толкованием вопросов распознавания лиц в Китае и тесно связано с исследованием данной статьи, рассмотрим подробнее его содержание. В Разъяснении всего 16 статей, которые касаются случаев злоупотребления технологией распознаванием лиц, применения вышеуказанной технологии, наступления деликтной ответственности, а также договорных правил и судебных процедур.

На практике некоторые приложения часто используют технологию распознавания лиц, чтобы сделать несущественную информацию об изображении лица необходимым условием для предоставления продуктов или услуг, без которой

---

[6] 中华人民共和国消费者权益保护法 [Закон КНР о защите прав потребителей]. URL: http://www.gov. cn/jrzg/2013-10/25/content_2515601.htm (дата обращения: 04.03. 2023).

[7] 中华人民共和国网络安全法 [Закон КНР о сетевой безопасности]. URL: http://www.npc.gov.cn/npc/c30834/201611/270b43e8b35e4f7ea98502b6f0e26f8a.shtml (дата обращения: 05.03. 2023).

[8] 中华人民共和国民法典 [Гражданский кодекс КНР]. URL: http://www.gov.cn/xinwen/ 2020-06/01/con tent_5516649.htm (дата обращения: 05.03.2023).

[9] 关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定 [О некоторых вопросах применения законодательства при рассмотрении гражданских дел, связанных с использованием технологии распознавания лиц при обработке персональных данных]. URL: http://www.hncourt.gov.cn/public/detail.php?id=187883 (дата обращения: 06.03.2023).

приложение не может быть установлено или использоваться; другие лица, обрабатывающие информацию, вынуждают или маскируют согласие физических лиц на обработку их информации об изображении лица, связывая его с другими разрешениями и другими способами. Такие принудительные запросы информации об изображении лица по замыслу приводят к тому, что физические лица не могут добровольно дать согласие на обработку информации об изображении лица или вынуждены соглашаться на обработку информации об изображении лица, которую они не хотят предоставлять и в которой нет необходимости. Доказательства, связанные с использованием технологии распознавания лиц, обычно находятся в руках обработчика информации. В сочетании с тем, что субъект информации не понимает, как обработчик информации ее обрабатывает, он сталкивается с барьером для доказывания того, что поведение обработчика информации является незаконным. Поэтому п. 2 ст. 6 Разъяснения предусматривает, что, «если обработчик информации утверждает, что его поведение соответствует обстоятельствам, указанным в пункте 1 статьи 1035 Гражданского кодекса, он несет бремя доказывания фактов, на которых оно основано». Статья 8 Разъяснения поясняет, что «разумные расходы, оплаченные потерпевшим лицом для прекращения нарушения, и разумные гонорары адвокатов могут быть востребованы в качестве имущественного ущерба».

В связи с разрозненностью потерпевших лиц на практике, высокой стоимостью защиты личных прав и ограниченной способности к доказыванию случаев, когда физические лица подают иски в защиту своих прав, относительно немного, и институт судебных разбирательств в защиту общественных интересов может эффективно восполнить этот недостаток. В свете практики народных судов по рассмотрению гражданских исков в защиту общественных интересов, касающихся персональных данных, статья 14 Разъяснения предусматривает гражданские иски в защиту общественных интересов, касающиеся информации об изображении лица.

Статья 26 Закона КНР «О защите персональных данных»[10] гласит: «Установка оборудования для сбора изображения лица и идентификации личности в общественных местах должна быть необходима для поддержания общественной безопасности, соответствовать соответствующим государственным нормам и устанавливать заметные напоминающие знаки». Учитывая, что технология распознавания лиц играет большую роль в профилактике и борьбе с эпидемиями, поиске пропавших детей, борьбе с незаконными преступлениями и поддержании общественной безопасности, ст. 5 Разъяснения устанавливает обстоятельства, когда обработчик информации не несет гражданской ответственности, например, если обработка информации об изображении лица ведется в целях реагирования на чрезвычайные ситуации в области здравоохранения или защиты жизни, здоровья и имущества физических лиц в чрезвычайных ситуациях.

На практике в КНР некоторые управляющие компании, которые обслуживают многоквартирные дома, в принудительном порядке требуют от жителей вводить информацию о своем изображении лица и используют технологию распознавания лиц как единственный способ проверки доступа в жилой комплекс, что нарушает принцип информированного согласия и вызывает вопросы со стороны общественности. В ст. 2 Разъяснения определены несколько типов наиболее распространенных действий, подпадающих под категорию действий против прав

[10] 中华人民共和国个人信息保护法 [Закон КНР о защите персональных данных]. URL: http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml (дата обращения: 05.03.2023).

и интересов личности физических лиц. К ним относятся в том числе использование технологии распознавания лиц для проверки, идентификации или анализа лиц в гостиницах, торговых центрах, банках, вокзалах, аэропортах, стадионах, развлекательных заведениях и других деловых помещениях и общественных местах в нарушение положений законов и административных правил. Информация об изображении лица относится к чувствительным персональным данным, и сбор и использование такой информации должны быть согласованы с жителем жилого помещения в соответствии с законом. Только если житель добровольно соглашается на использование системы распознавания лиц, сбор и использование информации о нем будет иметь правовую основу. Управляющие компании не могут использовать интеллектуальное управление как основание для ущемления прав личности соответствующих жителей. Поэтому п. 1 ст. 10 Разъяснения предусматривает, что, если управляющая компания использует технологию распознавания лиц в качестве единственного средства проверки для жителей для входа или выхода из зоны обслуживания компании, а житель не согласен и просит предоставить другие разумные средства проверки, народный суд должен поддержать его в соответствии с законом.

В последние годы частота преступлений против персональных данных граждан возросла, они серьезно нарушают безопасность персональных данных граждан и часто тесно связаны с другими преступлениями, такими как телекоммуникационное мошенничество, что приводит к все более заметной общественной опасности. Уголовно-правовая защита персональных данных граждан имеет прогрессивный характер развития. Поправки к Уголовному кодексу КНР (далее — УК КНР) от 28.02.2009 г.[11] впервые квалифицировали незаконное приобретение, продажу и предоставление персональных данных граждан как преступление, с тех пор появилась практика в сфере уголовно-правовой защиты персональных данных граждан, но в то время субъектом преступления были только сотрудники государственных органов или специальных подразделений. Поправки к УК КНР от 29.08.2015 г.[12] и введение ст. 253-1 расширяют субъектный состав преступления до общего субъекта, при этом специальный статус становится отягчающим обстоятельством для совершения данного преступления.

Судебный комитет Верховного народного суда и Прокурорский комитет Верховной народной прокуратуры 1 июня 2017 г. опубликовал Разъяснение «О некоторых вопросах применения законодательства при рассмотрении уголовных дел, связанных с нарушением персональных данных граждан»[13]. Разъяснение состоит из десяти статей, которые в основном определяют объем персональных данных граждан; критерии для осуждения и вынесения приговора за преступления против персональных данных граждан; вопросы снисхождения и отягчающих обстоятельств, конкурирующих преступлений, связанных с преступлениями против персональных данных граждан, и т. д.

---

[11] 中华人民共和国刑法修正案（七）[Поправки к Уголовному кодексу КНР от 28.02.2009г. № 10]. URL: http://www.npc.gov.cn/zgrdw/huiyi/cwh/1107/2009-02/28/content_1476563.htm (дата обращения: 05.03.2023).

[12] 中华人民共和国刑法修正案（九）[Поправки к Уголовному кодексу КНР от 29.08.2015 г. № 30]. URL: http://www.npc.gov.cn/zgrdw/npc/xinwen/2015-08/31/content_1945587.htm (дата обращения: 05.03.2023).

[13] 关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释 [Разъяснение о некоторых вопросах применения законодательства при рассмотрении уголовных дел, связанных с нарушением персональных данных граждан]. URL: https://www.spp.gov.cn/xwfbh/wsfbt/201705/t20170509_190088.shtml (дата обращения: 05.03.2023).

Также в КНР с 2012 г. государственные органы начали уделять особое внимание стандартизации в области защиты персональных данных. Так, Национальный технический комитет по стандартизации информационной безопасности обнародовал Руководство по государственному стандарту №GB/Z 28828-2012 «О защите персональных данных в информационных системах государственных и коммерческих служб с использованием технологий информационной безопасности»[14]. Данное Руководство является первым национальным стандартом по защите персональных данных в Китае.

Далее в 2020 г. была обнародована новая редакция Руководства по государственному стандарту №GB/T 35273-2020 «Технология информационной безопасности — Спецификации безопасности персональных данных»[15], где определены принципы и требования безопасности, которым необходимо следовать при осуществлении деятельности по обработке персональных данных. Руководство применяется к регулированию деятельности по обработке персональных данных различных типов организаций, а также к надзору, управлению и оценке деятельности по обработке персональных данных компетентными регулирующими органами, агентствами по оценке и другими организациями. Данный стандарт впервые проводит различие между персональными данными и чувствительными персональными данными, определяет виды персональных данных, классифицирует биометрические персональные данные, включая признаки распознавания лиц (чувствительные персональные данные), и устанавливает принципы информированного согласия, минимально достаточного использования и четкого разрешения на повторную передачу чувствительных персональных данных для сбора, хранения и использования.

2. Пробелы в законодательном регулировании

Из приведенного выше видно, что законодатель приложил немало усилий для защиты информации об изображении лица, но технология распознавания лиц постоянно развивается, законы в определенном смысле отстают: в действующем законодательстве все еще есть некоторые недостатки, и в связи с этим в настоящем разделе статьи предлагаем внести улучшения.

2.1. Неразработанность правоприменительной практики

В настоящее время нормы о защите информации распознавания лиц в Китае относительно разрозненны. Они существуют в законах, постановлениях, ведомственных инструкциях, судебных толкованиях и нормативных документах. Отсутствует соответствующее специальное регулирование, нет четко детерминированных положений в законодательстве. Кроме того, не сложилась правоприменительная практика, в зависимости от компетентных органов могут быть несбалансированные и конкурирующие стандарты правоприменения. Следовательно, для того чтобы улучшить работоспособность правовых норм технологии распознавания лиц и точно предотвращать риски безопасности, вызванные

[14] 信息安全技术公共及商用服务信息系统个人信息保护指南 [О защите персональных данных в информационных системах государственных и коммерческих служб с использованием технологий информационной безопасности]. URL: http://cxyz.yangzhou.gov.cn/312/5799.html (дата обращения: 05.03.2023).

[15] 信息安全技术—个人信息安全规范 [Технология информационной безопасности — Спецификации безопасности персональных данных]. URL: https://www.ahstu.edu.cn/wlzx/info/1011/1478.htm (дата обращения: 05.03.2023).

новыми технологическими разработками, и управлять ими, необходимо как можно скорее разработать правовые нормы специально для защиты биометрической информации, такой как информация о лице, уточнить критерии определения незаконных обстоятельств и унифицировать стандарты правоприменения.

2.2. Неясность понятия «согласие» в процессе обработки персональных данных

С точки зрения гражданского права правила информированного согласия состоят из двух частей: правила уведомления и правила согласия. Независимо от того, основан ли акт обработки персональных данных на согласии физического лица, обработчик, в принципе, обязан информировать данное лицо (если иное не предусмотрено законом), а те, кто не делает этого или делает это с нарушением установленных правил и не получает согласия субъекта информации на обработку его персональных данных, несут гражданско-правовую ответственность. Бао Сяоли считает: «...поскольку информация о распознавании лиц отличается от общей личной информации, существует большая разница между ней и другой биометрической информацией, такой как отпечатки пальцев. Поэтому обработка информации о распознавании лиц должна подлежать специальному регулированию и должна придерживаться более строгого принципа согласия»[16]. В действительности законодатель принял это мнение во внимание и установил в ст. 29 Закона КНР «О защите персональных данных», что на обработку чувствительных персональных данных должно быть получено индивидуальное согласие. Если же в данном Законе указано, что необходимо согласие индивида на сбор информации, то нет никаких дополнительных разъяснений относительно того, имеет ли любой субъект право на сбор информации, требуется ли разрешение государственных органов перед сбором информации, какой уровень мер по сохранению информации принимается после сбора и имеет ли право субъект поручить третьему лицу обеспечить ее сохранение. Для того чтобы пресечь злоупотребление технологией, необходимо создать административную систему лицензирования сбора, обработки и сохранения информации о распознавании лиц. Кроме того, потребители часто находятся в слабом положении при получении услуг, что может легко привести к утрате принципа информированного согласия по форме. Следовательно, необходимо усовершенствовать обязательство по уведомлению и механизм получения согласия, определить объем «согласия» в рамках технологии распознавания лиц, является ли оно согласием на всю информацию или на ее часть, включает ли оно согласие на сбор и повторное распространение информации обработчиком информации. На практике технология распознавания лиц используется не только в таких важных областях, как платежи и хранение, но и в сферах контроля доступа и регистрации, однако права и обязанности обработчика информации в обоих случаях одинаковы, что является недостатком, так как очевидно, что чувствительная информация требует повышенного уровня защиты.

2.3. Неясные критерии классификации персональных данных

ГК КНР и Закон КНР «О защите персональных данных» являются основными законодательными актами для защиты персональных данных. Так, ГК КНР предусматривает защиту частной жизни и персональных данных в разделе 6 «Личные

[16] 包晓丽. 数据共享的风险与应对 // 上海政法学院学报（法治论丛）.2021.№ 5.页129 [*Бао Сяоли.* Риски и меры реагирования на обмен данными // Вестник Шанхайского политико-правового института (серия о верховенстве права). 2021. № 5. С. 129].

права». Статья 1034 ГК КНР делит персональные данные на конфиденциальные и неконфиденциальные, причем положения о праве на частную жизнь применяются в первую очередь к конфиденциальным данным, а положения, касающиеся защиты персональных данных, применяются к неконфиденциальным данным и конфиденциальным данным, не предусмотренным положениями о праве на частную жизнь. Однако в главе 2 Закона КНР «О защите персональных данных» принято разделение на чувствительные и нечувствительные персональные данные. Руководство по государственному стандарту от 06.03.2020 г. №GB/T 35273-2020 «Технология информационной безопасности — Спецификации безопасности персональных данных» также использует термин «чувствительные персональные данные». В связи с этим возникает вопрос о том, приравнивается ли термин «чувствительные персональные данные» к термину «конфиденциальные персональные данные», существует ли перекрестная связь между ними и как она должна применяться.

2.4. Неясные стандарты для криминализации нарушения сбора информации об изображении лица

В Разъяснении «О некоторых вопросах применения законодательства при рассмотрении уголовных дел, связанных с нарушением персональных данных граждан» от 1 июня 2017 г. содержатся более подробные и конкретные положения о защите персональных данных. Так, ст. 5 Разъяснений дает перечень обстоятельств, когда незаконные приобретение, продажа или предоставление персональных данных граждан считаются тяжкими преступлениями и наказывается согласно ст. 253-1 УК КНР. Сюда относятся, например, незаконное приобретение, продажа или предоставление более 50 единиц информации о местонахождении и траектории движения, содержании связи, кредитной информации и информации о собственности; незаконное приобретение, продажа или предоставление более 500 единиц персональных данных граждан, такой как информация о жилье, записи о связи, медицинская и физиологическая информация, информация о сделках и другие персональные данные, которые могут повлиять на личную или имущественную безопасность; незаконное приобретение, продажа или предоставление более 5000 единиц персональных данных граждан, кроме указанных выше; повторное незаконное получение, продажа или предоставление персональных данных граждан; другие обстоятельства. К особо тяжким относятся деяния, когда в результате незаконных операций с персональными данными наступили тяжкие последствия, такие как смерть, серьезное увечье, психическое расстройство или похищение жертвы; значительный экономический ущерб или неблагоприятные социальные последствия; другие обстоятельства.

Из вышеизложенного видно, что ст. 5 Разъяснений делит персональные данные на три категории в зависимости от чувствительности их содержания и соответствующих норм криминализации. Норма криминализации для «информации о местонахождении и траектории движения, содержании связи, кредитной информации и информации о собственности» составляет более 50 единиц. Норма криминализации для «информации о жилье, записи о связи, медицинской и физиологической информации, информации о сделках и других персональных данных, которые могут повлиять на личную или имущественную безопасность», составляет более 500 единиц. Норма криминализации для «персональных данных граждан, кроме указанных в пунктах, составляет более 5000 единиц. Однако «биометрические персональные данные» не включены в классификацию, что приводит к нечеткому стандарту для инкриминирования информации об изображении лица. Если

информация об изображении лица будет интерпретироваться как «медицинская и физиологическая информация», это приведет к путанице, так как в Руководстве по государственному стандарту «Технология информационной безопасности — Спецификации безопасности персональных данных» «биометрические персональные данные» перечисляются наряду с «медицинской и физиологической информацией», причем параллельно, т. е. между ними нет ни включения, ни пересечения. Если трактовать информацию о изображении лица как «другие персональные данные, которые могут повлиять на личную или имущественную безопасность», и степень криминализации для таких данных будет составлять более 500 единиц, то, учитывая уникальные атрибуты информации об изображении лица и общественный вред от деяния незаконного приобретения, продажи или предоставления информации об изображении лица, такая трактовка не соответствует ее общественному вреду и сужает сферу посягательства на информацию об изображении лица. Поэтому в настоящее время, когда незаконное приобретение, продажа и предоставление информации об изображении лица стало весьма распространенным видом преступлений, уголовное законодательство срочно нуждается в уточнении конкретных и четких критериях криминализации деяний о незаконном использовании информации об изображении лица.

3. Способы предупреждения рисков и предложения по совершенствованию законодательства

Технология распознавания лиц работает по принципу хранения предварительно собранных биологических персональных данных в базе данных и сопоставления их с информацией при конкретном использовании. Однако поскольку лицо обладает уникальными и неизменяемыми характеристиками, после утечки информации невозможно полностью устранить негативные последствия с помощью традиционных методов, таких как сообщение о потере, составление и смена паролей. Информация о распознавании лиц затрагивает множество законных интересов, таких как личные права, право собственности и общественная безопасность, и ей необходимо уделять особое внимание. Согласно ст. 28 Закона КНР «О безопасности данных» осуществление деятельности по обработке данных, а также исследование и разработка новых технологий обработки данных должны способствовать экономическому и социальному развитию, повышению благосостояния людей и соответствовать общественной морали и этике. Стремление к достижению полезных целей с помощью технологий стало тенденцией развития нового века. Риски, возникающие при использовании технологии распознавания лиц, должны быть устранены путем сочетания технических усовершенствований и законодательных улучшений.

3.1. Уточнение классификации информации для распознавания лиц

Ввиду проблем, возникающих из-за различных классификаций персональных данных в ГК КНР и Законе КНР «О защите персональных данных», а также и в Руководстве по государственному стандарту «Технология информационной безопасности — Спецификации безопасности персональных данных», судебному департаменту следует издать более подробное толкование для детального разъяснения противоречий в законе. Хотя в уголовном законодательстве принята более уточненная классификация персональных данных граждан, основанная на принципе законности, в действующем уголовном законодательстве отсутствует информация

об изображении лица в рамках технологии распознавания лиц, что свидетельствует о наличии законодательного пробела. Информация об изображении лица при утечке, незаконном предоставлении или злоупотреблении приведет к тому, что субъект информации потеряет возможность контролировать объем распространения информации, что может вызвать значительные неконтролируемые риски, например при открытии банковских счетов, приобретении сим-карт и т. д. В связи с этим информация об изображении лица должна относиться к категории особо чувствительных персональных данных, а критерии криминализации должны быть применены и четко прописаны в законе.

3.2. Совершенствование административных правил и внедрение управления в соответствии с классификацией

В условиях широкого применения технологии распознавания лиц в коммерческой деятельности и в быту очень актуально совершенствование механизма административно-правовой защиты. Прежде всего следует создать специальный административный надзорный орган по защите персональных данных, уточнить границы полномочий и ответственности, чтобы избежать проблемы одновременного надзора со стороны нескольких учреждений, не сотрудничающих друг с другом и имеющих несогласованные стандарты правоприменения. Что касается административно-правовой защиты, следует определить право надзорного органа пересматривать, санкционировать, расследовать, инспектировать, отдавать приказы и осуществлять вмешательство в поведение различных субъектов при обработке персональных данных, а также право разрешать споры и право принимать жалобы и апелляции[17]. Вместе с тем надзорным органам необходимо участвовать в надзоре, управлении и оказании помощи для защиты прав и интересов сторон по многим аспектам. Организациями, работающими с конфиденциальными данными или неконфиденциальными данными и их совокупностью, нужно управлять в соответствии с категориями, и управление должно отличаться от управления организаций, специализирующихся на хранении информации. Конкретные способы классификации заключаются в следующем: для организаций, обладающих только неконфиденциальными персональными данными, должен быть принят режим регистрации, чтобы облегчить обработку персональных данных; а для организаций, обладающих только конфиденциальными персональными данными или как конфиденциальными, так и неконфиденциальными персональными данными, должно быть получено разрешение соответствующих государственных органов, чтобы проверить, имеет ли технический обработчик условия для хранения информации, особенно это касается тех организаций, которые собирают конфиденциальные персональные данные, включая информацию об изображении лица, — они должны быть уполномочены законом и иметь соответствующую квалификацию, т. е. технические средства и условия. Профессиональным хранителям персональных данных необходимо строго соответствовать лицензии и ежегодно проводить оценку рисков для предотвращения угрозы личной, общественной или национальной информационной безопасности. Система распознавания лиц должна регулярно тестироваться независимым профессиональным учреждением для определения ее точности, и при необходимости результаты регулярного тестирования должны быть представлены в надзорный орган.

[17] 付微明. 个人生物识别信息民事权利诉讼救济问题研究 // 法学杂志.2020.№ 3.页74 [*Фу Вэймин.* Исследование вопросов облегчения судебных разбирательств по гражданским правам в отношении личной биометрической информации // Журнал права. 2020. № 3. С. 74].

3.3. Создание динамичного механизма «согласия»

Чтобы реализовать принцип «информированного согласия» и избежать таких проблем, как общая авторизация и постоянная авторизация в конкретных сценариях применения распознавания лиц, очень важно создать динамичный механизм «согласия». С этой целью в законодательстве должно быть четко определено, что при изменении ключевых факторов, влияющих на риск, таких как цель сбора, сфера применения, методы и условия обработки, а также предмет хранения информации, субъект информации по распознаванию лиц должен быть своевременно уведомлен и предоставить новое согласие. Субъект информации о распознавании лиц имеет право отозвать согласие и воспользоваться правом на удаление информации. Организации, специализирующиеся на хранении информации, должны удалять соответствующие данные в течение определенного периода времени, под контролем независимой стороны. Следует установить общее запретительное положение на сбор информации, отличной от биометрической информации об изображении лица при применении технологии распознавания лиц, а если такой сбор необходим, следует потребовать отдельного согласия заинтересованного лица, а также проинформировать о соответствующих рисках и юридической ответственности.

Представляется, что, если одна и та же организация обладает только конфиденциальными персональными данными или совокупностью конфиденциальных и неконфиденциальных персональных данных, ей в принципе должно быть запрещено хранить эти данные на другой независимой платформе без согласия заинтересованного лица. Такая ситуация относительно часто встречается на практике. Например, китайский интернет-магазин Taobao обладает конфиденциальными персональными данными потребителей в связи с оплатой лицом и информацией о поведении потребителей в связи с записью потребления и следом просмотра, в этом случае обработчик информации должен нести ответственность за хранение информации. Несомненно, что хранение информации на другой независимой платформе в эпоху больших данных станет необходимостью и большое количество предприятий неизбежно будут передавать информацию квалифицированной организации для хранения. В этом случае Правила информированного согласия должны быть полностью реализованы в этом процессе и должно быть создано положение об «информированном согласии» для хранения информации на другой независимой платформе, чтобы своевременно информировать заинтересованное лицо о правах хранения информации на другой независимой платформе и соответствующих рисках, а также получить его согласие.

3.4. Улучшение технической поддержки и предоставление альтернативных вариантов

Организации, работающие с персональными данными, должны создать техническую систему отслеживания, чтобы впоследствии можно было проверить, кто, когда и где запрашивал, использовал, изменял или загружал информацию об изображении лица, чтобы в случае нарушения прав можно было провести расследование и найти нарушителя. Закон также должен предусматривать, что независимо от того, кто использует технологию распознавания лиц, если будет доказано, что собранные им персональные данные были украдены, произошла утечка, незаконные использование, продажа, предоставление и т. д., что привело к убыткам для субъекта персональных данных, обработчики будут нести солидарную ответственность за фактические убытки, понесенные жертвой.

Независимо от того, кто использует технологию распознавания лиц, люди имеют право отказаться от фотографирования их лиц. Если технология распознавания лиц используется в области неконкурентных услуг (например, в гражданской авиации, на железных дорогах, в школах, в жилых комплексах и т. д.), в случае отказа человека от фотографирования лица, работники этих мест должны предусмотреть другие альтернативные механизмы проверки и не могут отказать в пользовании услугой или доступе в зону обслуживания без фотографии лица.

Заключение

В эпоху стремительного развития больших данных широкое применение биометрической технологии распознавания лиц, несомненно, повысило эффективность и точность работы разных служб и организаций, но также возникло множество проблем, вызывающих реальные и потенциальные риски. Использование технологии распознавания лиц оказало влияние на традиционную систему защиты права гражданина на изображение и соответствующие законы должны быть усовершенствованы в этой связи. В данной статье проведен анализ применения технологии распознавания лиц и связанные с ней юридические риски, объясняется законодательная основа и недостатки в этой области в Китае, а также выдвигаются соответствующие предложения по дальнейшей защите информации об изображении гражданина в рамках технологии распознавания лиц. Только под двойной гарантией как продвижение развития технологии распознавания лиц и совершенствование законодательства можно обеспечить дальнейшую защиту права гражданина на изображение.

Статья поступила в редакцию 30 сентября 2023 г.
Рекомендована к печати 22 февраля 2024 г.

Legal protection of a citizen's right to a facial image when applying facial recognition technology in Chinese law

S. Jia, J. Zhang

For citation: Jia S., Zhang J. 2024. Legal protection of a citizen's right to a facial image when applying facial recognition technology in Chinese law. *Pravovedenie* 68 (2): 271–283. https://doi.org/10.21638/spbu25.2024.210 (In Russian)

In the era of the rapid development of big data, facial recognition biometric technology, which identifies and confirms the identity of persons by their face, is gradually becoming an object of public attention. Developing facial recognition technology has become an indispensable means of collecting information for government and commercial organizations. Facial recognition technology can be used to quickly identify individuals and improve efficiency and accuracy. However, there are two sides to everything, and the widespread use of facial recognition technology has affected the traditional system of protecting the citizen's right to a facial image, and the relevant laws should be improved in connection with the leakage and misuse of facial images. Only under the double safeguard, both the advancement of facial recognition technology and the improvement of laws can further protect the citizen's right to a facial image. This article analyzes the use of facial recognition technology and the risks associated with it, explains the legislative framework and its shortcomings in China, and makes appropriate proposals for further protection of the generated facial image information in facial recognition technology.

Keywords: face recognition technology, facial image protection, sensitive personal data, Chinese law, artificial intelligence, digitalization, personal rights, information.

References

Bao, Xiaoli. 2021. Risks and Responses to Data Sharing. *Journal of Shanghai Law School (Rule of Law Series)* 5: 122–136. (In Chinese)

Fu, Weiming. 2019. The legal protection model of personal biometric information and the choice of China. *Journal of East China University of Political Science and Law* 6: 78–88. (In Chinese)

Fu, Weiming. 2020. A Study on Litigation Remedies for Civil Rights of Personal Biometric Information. *Journal of Law* 3: 73–81. (In Chinese)

Hu, Ling. 2021. Swiping: Identity Regimes, Personal Information and Legal Regulation. *The Jurist* 2: 41–55. (In Chinese)

Jiang, Jie. 2019. Infringement risks and control strategies of face recognition technology applications. *Books & Intelligence* 5: 58–64. (In Chinese)

Miao, Jie. 2021. The Risk Challenges and Regulation of "Easy-to-Crack" Face. Recognition. *Information Security Research.* 10: 984–988. (In Chinese)

Received: September 30, 2023
Accepted: February 22, 2024

Shaoxue Jia — Dr. Sci. in Law, Shanghai University of Political Science and Law, 7989, Waiqingsong Road, Shanghai, 201701, China; ys02302041@126.com

Jingxin Zhang — Junior Researcher, Shanghai University of Political Science and Law, 7989, Waiqingsong Road, Shanghai, 201701, China; ys02302041@126.com