УДК 343.2/.7

ГАРАНТИИ ПРАВ ЛИЧНОСТИ В СИСТЕМЕ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

П.В. Пряжников, Д.В. Алонцева
Елецкий государственный университет им. И. А. Бунина
(Елец, Россия)

Резюме. Статья посвящена рассмотрению гарантий прав личности в системе обеспечения национальной безопасности в условиях цифровизации. Цель исследования – определить проблемы реализации прав личности в условиях построения цифровой среды. Авторами отмечено, что цифровые технологии сегодня играют ключевую роль в трансформации современного общества и формировании новых парадигм государственного управления, их внедрение в хозяйственную сферу и общественные отношения становятся мощным катализатором изменений, затрагивающих, в том числе сферу национальной безопасности. Внедрение цифровых технологий стимулирует процессы инновационного развития и модернизации общества, требуя адаптации его институтов и организационных структур к новым вызовам и возможностям, которые эти технологии предоставляют. Авторы поднимают проблему обеспечения прав личности, которые могут быть нарушены в результате обретения государством новых инструментов контроля над гражданами с целью предотвращения угроз национальной безопасности. Одним из таких инструментов является система видеонаблюдения в общественных местах, распространение и внедрение технологии распознавания лиц. Авторы приходят к выводу, что необходимо разработать более строгие и эффективные правовые механизмы для регулирования использования технологий распознавания лиц с целью обеспечения правопорядка. Это включает в себя установление четких правил сбора, хранения и использования биометрических данных, защиту личной жизни и принципов справедливого судебного процесса, а также контроль за деятельностью правоохранительных органов и предотвращение злоупотреблений.

Ключевые слова: права личности, национальная безопасность, система видеонаблюдения в общественных местах, технологии распознавания лиц

DOI 10.24888/2949-3293-2024-2-5-83-96

GUARANTEES OF INDIVIDUAL RIGHTS IN THE NATIONAL SECURITY SYSTEM IN THE CONTEXT OF DIGITALIZATION

Pavel V. Pryazhnikov, Dina V. Alontseva
Bunin Yelets State University
(Yelets, Russia)

Abstract. The article is devoted to the consideration of guarantees of individual rights in the system of ensuring national security in the context of digitalization. The purpose of the study is to identify the problems of realizing individual rights in the context of building a digi-

tal environment. The authors noted that digital technologies today play a key role in the transformation of modern society and the formation of new paradigms of public administration, their introduction into the economic sphere and public relations becomes a powerful catalyst for changes affecting, among other things, the sphere of national security. The introduction of digital technologies stimulates the processes of innovative development and modernization of society, requiring the adaptation of its institutions and organizational structures to new challenges and opportunities that these technologies provide. The authors raise the problem of ensuring the rights of the individual, which may be violated as a result of the acquisition by the state of new instruments of control over citizens in order to prevent threats to national security. One of these tools is a video surveillance system in public spaces, the dissemination and implementation of facial recognition technology. The authors conclude that it is necessary to develop stricter and more effective legal mechanisms to regulate the use of facial recognition technologies in order to ensure law and order. This includes establishing clear rules for the collection, storage and use of biometric data, protecting privacy and the principles of a fair trial, as well as monitoring the activities of law enforcement agencies and preventing abuse.

Keywords: personal rights, national security, video surveillance system in public places, facial recognition technologies

Цифровые технологии сегодня играют ключевую роль в трансформации современного общества и формировании новых парадигм государственного управления. Их внедрение в хозяйственную сферу и общественные отношения становится мощным катализатором изменений, затрагивающих, в том числе сферу национальной безопасности. Внедрение цифровых технологий стимулирует процессы инновационного развития и модернизации общества, требуя адаптации его институтов и организационных структур к новым вызовам и возможностям, которые эти технологии предоставляют. В рамках данного вопроса вызывает опасения проблема обеспечения прав личности, которые могут быть нарушены в результате обретения государством новых инструментов контроля над гражданами с целью предотвращения угроз национальной безопасности. Предметом широких дискуссий в научном сообществе долгое время остается вопрос видеонаблюдения в общественных местах, особенно в связи с распространением и внедрением технологии распознавания лиц. На сегодняшний день существует ряд пробелов в правовом регулировании технологий видеонаблюдения с функцией распознавания лиц, которые не могли не сказаться на правоприменительной практике.

Современные технологии распознавания лиц широко используются в биометрических системах для автоматического определения личности на основе уникальных физических, биологических или поведенческих особенностей. Наблюдается диспропорция в темпах развития разного рода цифровых технологий с возможностями правовой системы российского государства адаптироваться меняющимся условиям. На уровне правоприменительной практики возникает множество противоречий в определении того, что входит, по мнению ряда правоведов, в категорию биометрических персональных данных. Из этого следует невозможность выполнения всеми участниками реализации правовых установок своих должностных функций, исключая нарушение законных прав и интересов граждан.

Существующие нормы, регулирующие вопрос применения технологии распознания лиц, недостаточно конкретны, что создает препятствия для четкого их толкова-

ния и напрямую ведет к хаотичному, противозаконному использованию этих данных. Важно также учитывать, что технологии распознавания лиц могут быть применены для массового контроля за гражданами. Еще одной проблемой является недостаточная прозрачность в использовании и обработке данных, полученных с помощью систем распознавания лиц. Отсутствие четких правил хранения и доступа к этим данным может привести к их злоупотреблению и нарушению конфиденциальности граждан.

В настоящее время наблюдается тенденция к повсеместному внедрению систем распознавания лиц в разнообразных сферах общественной жизни. Очевидно, что данная тема становится предметом многочисленных дискуссий как в рамках научного сообщества, так и за его пределами, на социально-бытовом уровне. В данном контексте наблюдаются противоположные точки зрения. Сторонники подобных технологических новаций, в обоснование преимуществ технологий распознавания лиц, в первую очередь приводят аргументы о потенциальном сокращении числа преступных деяний [9, с. 121]. Однако сторонники иного подхода высказывают опасения относительно данной технологии, расценивая её как непосредственную угрозу гражданским правам.

Система распознавания лиц представляет собой технологию, позволяющую проводить сопоставление визуальных данных субъекта с цифровым изображением или видеоизображением, занесенным в специализированную базу. Данная технология, как правило, применяется в целях аутентификации, в точности измеряя черты лица по заданным параметрам. Предоставление доступа к системе распознавания лиц практически неизбежно влечет за собой возможные случаи злоупотреблений со стороны лиц, обладающих возможностью доступа к конфиденциальной информации.

На данный момент система стремительно совершенствуется и используется во многих странах. Применение систем видеонаблюдения в публичных местах не запрещено российским законодательством. Если это осуществляется в интересах государства или общества, на общественных мероприятиях или в общественных местах, то согласие гражданина на сбор, хранение, передачу и использование информации о его личной жизни не требуется. К таким местам относятся:

– транспортная инфраструктура (включая сеть дорог, железных дорог, водных путей, аэропортов, портов и других объектов, обеспечивающих передвижение людей, товаров и информации);

– места массового пребывания людей (торговые центры, стадионы, концертные площадки, парки, площади, а также общественные здания);

– объекты топливно-энергического комплекса (газопроводы, электростанции, атомные станции);

– гостиницы и иные объекты размещения людей;

– объекты в сфере культуры и другие территории.

Распространение данных технологий вызывает серьезные этические вопросы, особенно касающиеся защиты приватности граждан. Нарушение прав на приватность представляет риск, который включает возможность неправомерного раскрытия конфиденциальной информации. С развитием технологий частота атак со стороны хакеров увеличивается, что может привести к утечке личных данных, а также информации о местонахождении, социальных связях и привычках людей. Такие сведения могут стать объектом использования мошенниками, спецслужбами других стран или коммерческими организациями.

Дальнейшее развитие систем видеонаблюдения с распознанием лиц должно проводиться в строгих рамках государственного регулирования. При этом видеоизображения должны анализироваться с использованием базы данных, на доступ к которой имеют право только государство и граждане, выразившие согласие. Уведомление населения о работе системы распознания лиц является обязательным для обеспечения законности [3].

Таким образом, в настоящее время остро стоит проблема идентификации в цифровом пространстве с учетом обеспечения безопасности личных данных пользователей. С учетом стремительного развития данной технологии в короткий временной период, ученые высказывают опасения относительно сохранения эффективности правового регулирования. В особенности отмечается тот факт, что исследуемые системы используются, санкционируются и регламентируются органами государственной власти. Необходимо изучить правовые аспекты применения технологии правоохранительными органами государства, исследовать границы допустимого вмешательства должностных лиц в личную жизнь граждан [7, с. 80].

Правоохранительные органы применяют технологию распознания лиц непосредственно для реализации служебных предписаний, к ним может относиться, например, разыскивание преступников. На сегодняшний день многие города России оборудованы системами видеонаблюдения с опцией распознавания лиц. Это такие системы, как «Интегра-Видео-РЛ», «VisionLabs», аппаратно-программный комплекс «Безопасный город» (далее – АПК «Безопасный город») и др.

Основная цель комплекса заключается в собирании и анализе информации из различных подсистем, а также в координации их взаимодействия для достижения состояния защиты от угроз. При использовании баз данных правоохранительных органов системы видеонаблюдения автоматически выбирают записи с различных камер для идентификации подозреваемого лица. Городские системы видеонаблюдения обладают значительным потенциалом, обеспечивая оперативное получение информации для расследований и следственных мероприятий. Благодаря высокому качеству изображений и функциям распознавания лиц эти системы эффективно применяются в большинстве случаев.

Эти системы способны легко идентифицировать правонарушителя, что позволяет сотрудникам правоохранительных структур в короткие сроки определить местоположение искомого субъекта, произвести задержание. Также фото и видео, сделанные данными системами, могут быть использованы как средство документирования совершенного деяния. Большое значение состоит и в осуществлении превентивной функции. Упоминание о работе систем видеонаблюдения, особенно с функцией распознавания лиц, оказывает психологическое воздействие на граждан, стимулируя их к более сдержанному и законопослушному поведению из-за ожидания возможной идентификации личности. По мнению сотрудников МВД России, внедрение таких систем в городскую инфраструктуру способствует снижению уровня правонарушений. Видеомониторинг, особенно в криминогенных зонах, не только обеспечивает оперативное раскрытие преступлений, но и предотвращает их совершение в реальном времени [7, с. 84].

Ховавко С. М. отмечает, что в последние годы быстрое развитие технологий искусственного интеллекта и биометрической идентификации привело к возникновению

новых перспективных методов и технических средств для идентификации личности на основе биометрических данных. [10].

Определение биометрических данных в соответствии со статьей 11 Федерального закона «О персональных данных» включает в себя информацию, относящуюся к физиологическим особенностям человека, таким как рост, вес, цвет волос, группа крови, а также данные об отпечатках пальцев и другие сведения, которые могут быть использованы для идентификации личности [2]. Биометрические данные могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных.

Таким образом, в работе правоохранительных органов значительное внимание уделяется техническим средствам, позволяющим осуществить распознание лица. Предполагается, что данная технология находится на этапе постепенного внедрения в работу органов правоохраны и будет использоваться еще более интенсивно с развитием правовых основ, материально-технического обеспечения данного процесса. Данная технология успешно применяется в расследовании преступлений, их пресечении, предотвращении массовых беспорядков и в иных целях. В настоящее время наблюдается активное законодательное стремление к расширению области применения биометрической регистрации. Это включает предложения о возможности получения различных государственных услуг после прохождения процедуры биометрической регистрации, включая услуги, предоставляемые в многофункциональных центрах «Госуслуги».

Современное общество стоит перед историческим вызовом, связанным с масштабным переходом к новой технологической парадигме. Этот переход предполагает не только изменения в технических аспектах, но также значительную перестройку общественных институтов. Этот процесс затрагивает организацию общества, системы управления и ценностные ориентации. Взаимодействие между людьми прямо зависит от технологий, которые используются для этого, и поэтому важно глубоко понимать роль техники в социальных процессах. Научно-технический прогресс создает ряд этических и ценностных проблем, которые требуют оперативного правового реагирования или, по крайней мере, опережающего его.

На сегодняшний день в Российской Федерации ключевым законом, закрепляющим правовые основы регулирования распознавания лиц, является Федеральный закон от 29 декабря 2022 г. N 572-ФЗ «Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации» [8].

Важно упомянуть также роль Конституции Российской Федерации в данном вопросе. Основной закон напрямую не закрепляет применение системы распознавания лиц, однако отдельные статьи, такие как часть 1 статьи 23, защищают право каждого гражданина на неприкосновенность частной жизни, личную и семейную тайну, а статья 24 запрещает обработку информации о частной жизни лица без его согласия, за исключением следственных действий и оперативно-розыскных мероприятий [1].

Однако необходимо признать, что указанные документы не регулируют в полной мере все аспекты, связанные с использованием городских систем видеонаблюдения в целом и систем видеонаблюдения с функцией распознавания лиц, в частности.

Правительство Российской Федерации утверждает форму согласия на размещение и обработку персональных данных в единой системе идентификации и аутентификации, а также биометрических персональных данных в единой биометрической системе. Физическое лицо имеет право подписать данное согласие усиленной неквалифицированной электронной подписью. Отсутствие должного законодательного регулирования данной сферы вызывает опасения в сообществах ученых, экспертов и практиков не только в РФ, но и во всем мире. На данный момент острыми является ряд вопросов: об ответственности граждан и государств за пресечение границ невмешательства в частную жизнь иных лиц, об определении сущности понятий «персональные данные», «идентификация», «биометрические данные» и т.д.

Вопрос о введении специального регулирования для новых категорий персональных данных, например, биометрической информации, вызывает различные точки зрения в научной литературе. В отечественных исследованиях отсутствует единство мнений относительно необходимости и целесообразности выделения биометрических данных в отдельную категорию персональных данных.

По мнению Е. Покаместовой, введение специальных норм, регулирующих обработку биометрических персональных данных в российском законодательстве, не является обоснованным, так как более целесообразным представляется включение их в одну из уже существующих категорий персональных данных [54, с. 32]. С развитием информационных технологий и увеличением объема обрабатываемых персональных данных возникает дискуссия о применении объективного и субъективного подходов к обработке таких данных. Под объективным подходом понимается признание информации персональными данными независимо от возможности оператора провести идентификацию субъекта. По субъективному подходу, оператор должен обладать разумными средствами для определения личности субъекта на основе дополнительной информации, имеющейся у него или полученной от других лиц.

В России на данный момент активно осуществляется внедрение системы распознавания лиц в рамках реализации проекта «Безопасный город». Этот проект предусматривает использование комплекса программно-аппаратных средств и организационных мер для обеспечения видеоохраны и технической безопасности. Преимущественно такие системы развертываются в общественных местах, таких как аэропорты и станции метро, с целью обеспечения безопасности в транспортных узлах [10]. «Безопасный город» начал свою деятельность как система видеонаблюдения, но со временем был расширен различными функциональными модулями. Эта автоматизированная система разработана для обеспечения потребностей города в области безопасности и основана на комплексе программно-аппаратных средств и организационных мер для обеспечения видеоохраны и технической безопасности.

Основные цели комплекса заключаются в собирании и анализе информации, поступающей из различных подсистем, а также в координации их взаимодействия для обеспечения безопасности города. Информация с каждого объекта передается в центральный узел для хранения данных, где осуществляется их обработка и передача. Этот узел выполняет функции оцифровки видеоматериалов, преобразования аналогового сигнала, а также кратковременного хранения данных перед их передачей в оперативно-технический центр. В оперативно-техническом центре информация хранится на протяжении длительного времени. Полученные данные представляют собой краткие обзоры

событий, передающие основную суть происходящего и запоминая важные детали, включая изображения всех участников.

Такие «короткие» данные обладают преимуществом в мгновенном отображении на экране и немедленной передаче по назначению. При необходимости выявить нарушителя закона лицо на записях анализируется с использованием базы данных правоохранительных органов. Система автоматически подбирает соответствующие видеозаписи с различных камер наблюдения, идентифицируя подозреваемого на видео.

Таким образом, городские системы видеонаблюдения обладают значительным потенциалом. Их высокая скорость реагирования позволяет быстро получать информацию и использовать её при необходимости в оперативно-розыскных мероприятиях и следственных действиях. Благодаря высококачественным изображениям и функции распознавания лиц системы видеонаблюдения проявляют свою эффективность в 85-90 % случаев.

На данный момент в Российской Федерации отсутствует специальные нормативные акты, законодательно регулирующие вопрос использования технологий распознавания лиц.

Имеется информация, подтверждающая эффективность системы распознавания лиц со стороны Министерства внутренних дел Российской Федерации. Представители Главного управления МВД по городу Москве утверждают, что данная технология позволяет успешно выявлять и разыскивать преступников [6]. Рассмотрим анализ материалов судебной практики по данному вопросу.

Савеловский суд обнародовал мотивированную часть решения по делу № 02а-0577/2019, связанному с иском гражданки Москвы Алены Поповой. Она выдвигала требование о признании незаконного использования технологии распознавания лиц в системе видеонаблюдения [4]. Алена Попова утверждала, что обработка биометрических данных с видеокамер наблюдения без получения письменного согласия человека противоречит законодательству о персональных данных. Она требовала удалить свои биометрические персональные данные из базы данных изображений, включая Единый центр хранения данных (ЕЦХД). Однако Савеловский суд отклонил её иск. В своем исковом заявлении Алена Попова пояснила, что в апреле 2018 года она устроила одиночный пикет у здания Государственной Думы Российской Федерации.

Несмотря на отсутствие достаточных доказательств её вины в организации и проведении несанкционированного массового мероприятия, Тверской районный суд привлек её к административной ответственности и наложил штраф.

Постановление о привлечении к административной ответственности и наложении административного штрафа было впоследствии обжаловано в вышестоящих судах. Судом было отказано в удовлетворении заявленных требований в полном объёме на следующем основании: «Департамент получает и обрабатывает изображения в ЕЦХД, руководствуясь ст. 152.1 Гражданского кодекса РФ, устанавливающей, что согласие гражданина на обнародование и дальнейшее использование изображения гражданина (в том числе его фотографии, а также видеозаписи или произведения изобразительного искусства, в которых он изображён) не требуется в случаях, когда:

- использование изображения осуществляется в государственных, общественных или иных публичных интересах.

- изображение гражданина получено при съёмке, которая проводится в местах, открытых для свободного посещения, или на публичных мероприятиях (собраниях, съездах, конференциях, концертах, представлениях, спортивных соревнованиях и подобных мероприятиях), за исключением случаев, когда такое изображение является основным объектом использования».

Согласно решению Савеловского суда, система видеонаблюдения применяет технологии распознавания лиц, однако не предоставляет возможность установить личность конкретного человека.

Суд пришел к заключению, что «технология распознавания лиц не является запрещенным методом использования информации ее владельцем». Это набор видеоаналитических алгоритмов, представляющих собой совокупность организационно-технических мер и действий, направленных на разработку и применение технических решений для предоставления услуг с использованием Единого центра хранения данных (ЕЦХД) и соответствующих основным задачам пользователей данного центра.

В соответствии с федеральным законом № 152-ФЗ «О персональных данных» предусмотрена разумная степень свободы использования механизма «обработка персональных данных/изображения». Департамент использует этот механизм для достижения законных целей, поскольку «государство вправе самостоятельно выбирать наиболее эффективные средства защиты прав граждан», как указано в мотивировочной части решения суда. Согласно изложенному, в качестве оператора Единого центра хранения данных (ЕЦХД) Департамент обладает необходимыми законными основаниями для приема-передачи, хранения и обработки видеоинформации любым законным методом.

Суд определил, что сами видеоизображения не подпадают под категорию биометрических персональных данных, следовательно, не требуется получение письменного согласия от человека на их обработку. С другой стороны, на практике полиция имеет полное законное право обрабатывать персональные данные граждан и вносить полученную информацию в базы данных [66].

Таким образом, реализация на практике законодательства о распознавании лиц в РФ является несовершенной. В действительности, многие нормы противоречат друг другу и расходятся с правоприменительной практикой. Изучение судебной практики показывает, что с появлением данной технологии начали возникать резонансные прецеденты, связанные с нарушением гражданских и политических прав граждан Российской Федерации. В связи с этим в научном сообществе ведутся широкие дискуссии о границах использования властными структурами цифровых технологий, способных, фактически, «преследовать» отдельных граждан и их объединения за политическую позицию и взгляды, что противоречит установленным в Основном законе государства демократическим принципам. Рассмотрим подобный случай в зарубежной практике.

21 ноября 2019 г. Апелляционный суд Англии и Уэльса принял для рассмотрения жалобу жителя Кардиффа на решение нижестоящего суда, которое в сентябре текущего года признало законность правоохранительных служб Великобритании в использовании системы автоматического распознавания лиц (AFR) [5].

В исходном иске, поданном в суд Уэльса в мае того же года, отмечалось, что используемая технология сканирования лиц нарушает право граждан Великобритании на неприкосновенность частной жизни и нарушает законодательство в области защиты персональных данных.

«Мы проживаем не в авторитарном обществе, а в рамках демократии. Полиция приступила к использованию этой технологии против меня и тысяч других жителей моего района без предварительного уведомления или обсуждения», — подчеркивал заявитель Эд Бриджес. Адвокаты Бриджеса пояснили, что процесс сканирования лиц с последующим внесением биометрических данных в систему должен рассматриваться аналогично сбору ДНК или отпечатков пальцев без ведома или согласия человека, что представляет собой нарушение законодательства Великобритании. Однако ситуация усложняется отсутствием эффективного и соответствующего требованиям современности законодательного регулирования технологии AFR и её алгоритмов применения.

В полиции Южного Уэльса утверждали, что использование технологии AFR не нарушает прав граждан на неприкосновенность частной жизни и защиту данных. Они указывали, что данная технология аналогична любому снимку человека на камере в общественных местах, и полученные данные удаляются с серверов правоохранительных органов в течение 31 календарного дня. Представители полиции также подчеркивали, что в настоящее время разрабатываются принципы работы AFR, которые будут сбалансированы с учетом безопасности и конфиденциальности.

В Государственном департаменте США работает одна из крупнейших в мире систем распознавания лиц с базой данных из 117 миллионов взрослых американцев, фотографии которых обычно взяты из фотографий водительских прав. Хотя она все еще далека от завершения, ее используют в некоторых городах, чтобы дать представление о том, кто был на фотографии. ФБР использует фотографии как инструмент расследования, а не для положительной идентификации. По состоянию на 2016 год, распознавание лиц использовалось для идентификации людей на фотографиях, сделанных полицией в Сан-Диего и Лос-Анджелесе (не на видео в реальном времени, а только на фотографиях).

ФБР также внедрило свою программу идентификации следующего поколения, включающую распознавание лиц, а также более традиционные биометрические данные. Это отпечатки пальцев и сканирование радужной оболочки, которые могут быть получены как из уголовных, так и из гражданских баз данных. Федеральное управление общей подотчетности раскритиковало ФБР за то, что оно не решило различные проблемы, связанные с конфиденциальностью и точностью.

Начиная с 2018 года, таможня и пограничная служба США внедрили «биометрические сканеры лица» в аэропортах США. Пассажиры, вылетающие международными рейсами, могут пройти регистрацию, проверку безопасности и посадку после получения изображений лиц и проверки их соответствия фотографиям, удостоверяющим личность, хранящимся в базе данных [12]. Изображения, сделанные путешественниками с гражданством США, будут удалены в течение 12 часов. Управление транспортной безопасности (TSA) выразило намерение внедрить аналогичную программу для внутренних авиаперевозок в процессе проверки безопасности в будущем. Американский союз защиты гражданских свобод является одной из организаций, выступающих против программы, поскольку программа будет использоваться в целях слежки.

В 2006 году китайское правительство инициировало проект Skynet по внедрению систем видеонаблюдения по всей стране, и по состоянию на 2018 год для этого проекта по всей стране было развернуто 20 миллионов камер, многие из которых способны распознавать лица в режиме реального времени. В 2017 году полиция Циндао

смогла идентифицировать двадцать пять разыскиваемых подозреваемых с помощью оборудования для распознавания лиц на Международном фестивале в Циндао, один из которых был в бегах в течение 10 лет [11].

В конце 2017 года Китай внедрил технологии распознавания лиц и искусственного интеллекта в Синьцзяне. Репортеры, посетившие регион, обнаружили камеры наблюдения, установленные примерно через каждые сто метров в нескольких городах, а также контрольно-пропускные пункты распознавания лиц в таких местах, как заправочные станции, торговые центры. В феврале 2020 года, после вспышки коронавируса, Megvii обратилась за банковским кредитом для оптимизации системы скрининга температуры тела, которую она запустила, чтобы помочь выявлять людей с симптомами коронавирусной инфекции в толпе.

Многие общественные места в Китае оснащены оборудованием для распознавания лиц, включая железнодорожные вокзалы, аэропорты, туристические достопримечательности, выставки и офисные здания. В октябре 2019 года профессор Чжэцзянского научно-технического университета подал в суд на сафари-парк Ханчжоу за злоупотребление личной биометрической информацией клиентов. Сафари-парк использует технологию распознавания лиц для проверки личности владельцев своих годичных карточек [14].

Применение системы распознавания лиц является фактором социального беспокойства даже в развитых технологичных странах. Китай является ярким примером, поскольку в 2019 году протестующие в Гонконге разрушили умные фонарные столбы из-за опасений, что на них могут быть установлены камеры и система распознавания лиц, используемые китайскими властями для наблюдения.

Таким образом, как показывает изученная информация, судебная практика зарубежных государств также не является совершенной. Некоторые государства вводят ограничения на применение технологии распознавания лиц в связи с нарушением гражданских свобод населения. Другие же страны, в частности Китай, внедряют данную технологию в самые разнообразные сферы общественной жизни, используют как инструмент контроля над населением страны. Данный факт выступает катализатором роста социальной напряженности, что нарушает политическую стабильность.

Государство, в основе которого лежат права человека и свобода личности, прежде всего, должно гарантировать надежные способы шифрования и последующего уничтожения информации. Следовательно, реализация на практике данного принципа зависит напрямую от идеологии государственной власти. Авторитарные государства получают возможность, собирая информацию о гражданах, напрямую следить за ними через различные системы.

Исследование научной группы Кембриджского университета выявило, что использование систем распознавания лиц в реальном времени (LFR) полицией Великобритании не соответствует минимальным этическим и правовым стандартам. Ученые проанализировали применение данной системы правоохранительными органами Лондона и их коллегами в Южном Уэльсе при помощи собственного инструмента аудита.

Исследователи пришли к выводу, что использование технологии LFR следует полностью исключить. Система сравнивает лица, снятые с камер, с фотографиями из базы данных для выявления совпадений. Некоторые авторитарные страны применяют данную технологию в качестве инструмента государственного контроля над граждан-

ским населением. В 2020 году полиция Великобритании начала испытывать данную систему с целью борьбы с преступностью и терроризмом. Правоохранители использовали технологию LFR для сканирования толпы с целью выявления преступников, находящихся в списке наблюдения.

Группа исследователей обнаружила, что полиция утаивала информацию об использовании данной системы. «В то же время отсутствуют надежные механизмы компенсации ущерба, причиненного отдельным лицам и сообществам, пострадавшим от применения правоохранителями этой технологии», – заявила главная автор исследования Эвани Радия-Диксит. Тем не менее, она отметила, что полицейские не обязаны нести ответственность за ущерб, вызванный использованием технологии распознавания лиц [13].

Исследователи выявили проблемы в функционировании системы, связанные с расовым профилированием и отсутствием эффективных механизмов ответственности за её использование. В июле правительство Великобритании отклонило предложение комитета юстиции и внутренних дел Палаты лордов относительно применения полицией системы распознавания лиц [13].

Анализ как отечественной, так и зарубежной практики показал, что вопрос распознавания лиц осложняется отсутствием эффективной и отвечающей запросам сегодняшнего дня нормативной базы для регулирования технологии. В современном обществе распознание лиц в целях обеспечения правопорядка представляет собой актуальную проблему, которая требует серьезного правового регулирования. Основной задачей такого распознавания является идентификация подозреваемых лиц или лиц, совершающих правонарушения, с целью предотвращения преступлений, обеспечения безопасности общества и установления правосудия. Однако, несмотря на потенциальные выгоды, использование технологий распознавания лиц вызывает ряд серьезных проблем с точки зрения правового регулирования.

Одной из основных проблем является вопрос о защите личных данных граждан. Распознавание лиц может включать в себя сбор и хранение большого объема биометрических данных, таких как изображения лиц, которые могут быть рассмотрены как чувствительная личная информация. Это вызывает опасения относительно возможности злоупотребления этой информацией и нарушения прав на приватность граждан.

Второй проблемой является потенциальное нарушение принципа презумпции невиновности. При использовании технологий распознавания лиц существует риск ложных срабатываний, когда невиновные люди могут быть ошибочно идентифицированы как преступники. Это может привести к неправомерному преследованию и ограничению прав таких лиц.

Третья проблема связана с отсутствием четких норм и стандартов в области использования и хранения биометрических данных. В некоторых случаях правовые рамки могут быть недостаточно развитыми или неоднозначными, что может привести к произволу со стороны уполномоченных органов и нарушению законных прав граждан.

Четвертая проблема состоит в возможности злоупотребления технологиями распознавания лиц для массового слежения за гражданами и подавления политических свобод. Использование таких технологий государственными структурами может привести к созданию общества контроля и нарушению демократических принципов.

В целом, необходимо разработать более строгие и эффективные правовые механизмы для регулирования использования технологий распознавания лиц с целью обеспечения правопорядка. Это включает в себя установление четких правил сбора, хранения и использования биометрических данных, защиту личной жизни и принципов справедливого судебного процесса, а также контроль за деятельностью правоохранительных органов и предотвращение злоупотреблений.

Список литературы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // СПС «Консультант Плюс».
2. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 06.02.2023) «О персональных данных» // СПС «Консультант Плюс».
3. Постановление Правительства РФ от 16.07.2016 № 678 «О требованиях по обеспечению транспортной безопасности, в том числе требованиях к антитеррористической защищенности объектов (территорий), учитывающих уровни безопасности для различных категорий объектов транспортной инфраструктуры и транспортных средств морского и речного транспорта» // Собрание законодательства РФ. 2016. № 31. Ст. 5012.
4. Апелляционное определение Ульяновского областного суда по делу №22-374/2023 от 1 марта 2023 года в отношении Эбеккуева А.Х. – URL: http://www.uloblsud.ru/index.php?option=3&id=90&idCard=104961 (дата обращения 20.03.2024)
5. Решение Савёловского районного суда по делу 02а-0577/2019 в отношении Поповой А.В. – URL: https://mos-gorsud.ru/rs/savyolovskij/services/cases/kas/details/988f386e-be51-47b0-b48f-e871043ef1fc (дата обращения 16.03.2024)
6. Апелляционный суд Англии изучит законность использования системы распознавания лиц / Российское агентство правовой и судебной информации – РАПСИ https://rapsi-pravo.ru/international_news/20191121/305078513.html (дата обращения: 11.02.2024).
7. Гаврилов Б.Я. Правоохранительные органы России: учебник для вузов / Б. Я. Гаврилов [и др.] ; под общей редакцией Б. Я. Гаврилова. 7-е изд., перераб. и доп. Москва: Издательство Юрайт, 2024. 344 с. (Высшее образование). ISBN 978-5-534-16343-8. Текст : электронный // Образовательная платформа Юрайт [сайт]. URL: https://urait.ru/bcode/535422 (дата обращения: 11.02.2024).
8. Колоткина, О. А. Право личности на безопасность: понятие и механизмы обеспечения в РФ: теоретико-правовое исследование: дис. ... канд. юрид. наук: 12.00.01 / Колоткина Оксана Анатольевна; Саратов. гос. акад. права. Екатеринбург, 2009. 215 с.
9. Хазов Е.Н. Юридические гарантии прав и свобод человека и гражданина и механизм их реализации // Вестник Московского университета МВД России. 2017. № 5. С. 120-123.
10. Ховавко С. М. Теоретико-правовые и организационные основы технического отождествления личности на основе биометрической идентификации в оперативно-розыскной деятельности // Вестник Уральского юридического института МВД России.

2022. №2 (34). URL: https://cyberleninka.ru/article/n/teoretiko-pravovye-i-organizatsionnye-osnovy-tehnicheskogo-otzhdestvleniya-lichnosti-na-osnove-biometricheskoy-identifikatsii-v (дата обращения: 10.02.2024).

11. Суд отклонил иск москвички о признании незаконной системы распознавания лиц - РИА Новости, 06.11.2019 https://ria.ru/20191106/1560629920.html (дата обращения: 11.02.2024).

12. A lawsuit against face-scans in China could have big consequences. The Economist. November 9, 2019. – URL: https://www.economist.com/china/2019/11/09/a-lawsuit-against-face-scans-in-china-could-have-big-consequences (дата обращения 16.03.2024)

13. Face Recognition based Smart Attendance System Using IoT. International Research Journal of Engineering and Technology. 9 (3): 5. March 2022. – URL: https://www.irjet.net/archives/V9/i3/IRJET-V9I333.pdf (дата обращения 18.03.2024)

14. Radiya-Dixit, Evani. A Sociotechnical Audit: Assessing Police Use of Facial Recognition (Cambridge: Minderoo Centre for Technology and Democracy, 2022). – URL: https://doi.org/10.17863/CAM.89953 (дата обращения 18.03.2024)

References

1. Federal Law No. 152-FZ dated 07/27/2006 (as amended on 02/06/2023) «On Personal Data» // SPS Consultant Plus.

2. Decree of the Government of the Russian Federation dated 07/16/2016 No. 678 "On Requirements for ensuring transport security, including requirements for anti-terrorist protection of objects (territories) that take into account security levels for various categories of transport infrastructure facilities and sea and river transport vehicles" // Collection of legislation of the Russian Federation. 2016. No. 31. St. 5012.

3. The official statement of the Ulyanovsk Regional Court in case No. 22-374/2023 dated March 1, 2023 in respect of A.A. Bekkueva – URL: <url> http://www.uloblsud.ru/index.php?option=3&id=90&idCard=104961 (accessed 03/20/2024)

4. The statement of the Savlovsky District Court in the case 02a-0577/2019 on behalf of the President A.V. – URL: <url> https://mos-gorsud.ru/rs/savyolovskij/services/cases/kas/details/988f386e-be51-47b0-b48f-e871043ef1fc (accessed 03/16/2024)

5. The Court of Appeal of England will examine the legality of using the facial recognition system / Russian Agency for Legal and Judicial Information – https://rapsi-pravo.ru/international_news/20191121/305078513.html RAPSI (date of application: 02/11/2024).

6. Gavrilov B.Ya. Law enforcement agencies of Russia: textbook for universities / B. Ya. Gavrilov [et al.]; edited by B. Ya. Gavrilov. 7th ed., reprint. and add. Moscow : Yurait Publishing House, 2024. 344 p. (Higher education). ISBN 978-5-534-16343-8. Text : electronic // Educational platform [website]. https://urait.ru/bcode/535422 (date of appeal: 02/11/2024).

7. Khazov E.N. Legal guarantees of human and civil rights and freedoms and the mechanism of their implementation // Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2017. № 5. pp. 120-123.

8. Kolotkina, O. A. The right of the individual to security: the concept and mechanisms of security in the Russian Federation: theoretical and legal research: dissertation of the candidate. Jurid. sciences': 12.00.01 / Kolotkina Oksana Anatolyevna; Saratov State Academy of Sciences. rights. Yekaterinburg, 2009. – 215 p.

9. Suddenly I heard from a Muscovite about the appearance of an unknown warning system, 06.11.2019 https://ria.ru/20191106/1560629920.html (date of application: 02/11/2024).

10. A lawsuit against face scanning in China could have serious consequences. The economic crisis. November 9, 2019 – URL: https://www.economist.com/china/2019/11/09/a-lawsuit-against-face-scans-in-china-could-have-big-consequences (accessed 03/16/2024)

11. Intelligent attendance system based on face recognition using the Internet of Things. International Scientific Research Journal of Engineering and Technology. 9 (3): 5. March 2022. URL: https://www.irjet.net/archives/V9/i3/IRJET-V9I333.pdf (accessed 03/18/2024)

12. Radium-Dixit, Evani. Sociotechnical Audit: Assessment of the use of facial recognition techniques by the police (Cambridge: Minderu Center for Technology and Democracy, 2022). URL: https://doi.org/10.17863/CAM.89953 (accessed 03/18/2024)