

DOI: 10.17803/1729-5920.2022.183.2.121-131

Д. Л. Кутейников*,
О. А. Ижаев**,
В. А. Лебедев***,
С. С. Зенин****

Неприкосновенность частной жизни в условиях использования систем искусственного интеллекта для удаленной биометрической идентификации личности¹

Аннотация. В статье проанализированы правовые подходы к разрешению ключевых проблем реализации прав человека в условиях массовой эксплуатации в общественном пространстве систем искусственного интеллекта (ИИ). В рамках исследования акцент сделан на особенностях правовой регламентации применения систем искусственного интеллекта для удаленной биометрической идентификации личности. Применение данных систем в настоящее время только начинает обретать нормативную правовую базу и правоприменительную практику в большинстве стран. В исследовании проанализированы несколько различных моделей правового регулирования, которые характерны для отдельных стран и регионов, таких как Великобритания, США, КНР, ЕС и Россия.

В Великобритании допускается использование систем распознавания лиц в реальном времени в общественных пространствах, однако набор сценариев и ситуаций их использования существенно ограничен законодательством и правоприменительной практикой. В США как на федеральном, так и на уровне

¹ Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 18-29-16193.

© Кутейников Д. Л., Ижаев О. А., Лебедев В. А., Зенин С. С., 2022

* *Кутейников Дмитрий Леонидович*, кандидат юридических наук, доцент кафедры конституционного и муниципального права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)

Садовая-Кудринская ул., д. 9, г. Москва, Россия, 125993

kuteynikov@me.com

** *Ижаев Осман Аликович*, кандидат юридических наук, заместитель директора Института бизнес-права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)

Садовая-Кудринская ул., д. 9, г. Москва, Россия, 125993

izhaev.osman@gmail.com

*** *Лебедев Валериан Алексеевич*, доктор юридических наук, профессор, профессор кафедры конституционного и муниципального права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)

Садовая-Кудринская ул., д. 9, г. Москва, Россия, 125993

lebedev_va@bk.ru

**** *Зенин Сергей Сергеевич*, кандидат юридических наук, доцент, директор Института государства и права Тюменского государственного университета, проректор Тюменского государственного университета, доцент кафедры конституционного и муниципального права Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)

ул. Володарского, д. 6, г. Тюмень, 625003, Россия

zeninsergei@mail.ru

штатов отсутствуют общие нормы, формирующие единый правовой подход к регулированию рассматриваемой области. В ЕС разработан проект Регламента о гармонизированных правилах в отношении ИИ (Artificial Intelligence Act), которым предполагается установление запрета на использование систем ИИ для удаленной биометрической идентификации физических лиц в режиме реального времени в общедоступных местах. В КНР отсутствует специальное нормативное регулирование данной сферы общественных отношений. Развитие данных систем в КНР подконтрольно государству, что в силу высокой централизации власти приводит к риску нарушения прав человека и создания атмосферы тотальной слежки за гражданами без каких-либо законодательно установленных рамок и ограничений. В России государство активно разворачивает данные системы на федеральном и региональном уровнях при отсутствии специализированной нормативной правовой базы. Права человека защищены лишь общими нормами Конституции РФ и законодательства, правоприменительная практика направлена преимущественно на обеспечение интересов государства.

Ключевые слова: распознавание лиц; биометрическая идентификация; искусственный интеллект; неприкосновенность частной жизни; права человека; нематериальные блага.

Для цитирования: Кутейников Д. Л., Ижаев О. А., Лебедев В. А., Зенин С. С. Неприкосновенность частной жизни в условиях использования систем искусственного интеллекта для удаленной биометрической идентификации личности // Lex russica. — 2022. — Т. 75. — № 2. — С. 121–131. — DOI: 10.17803/1729-5920.2022.183.2.121-131.

Privacy in the realm of Artificial Intelligence Systems Application for Remote Biometric Identification²

Dmitriy L. Kuteynikov, Cand. Sci. (Law), Senior Lecturer, Department of Constitutional and Municipal Law, Kutafin Moscow State Law University (MSAL)
ul. Sadovaya-Kudrinskaya, d. 9, Moscow, Russia, 125993
kuteynikov@me.com

Osman A. Izhaev, Cand. Sci. (Law), Deputy Director, Business Law Institute, Kutafin Moscow State Law University (MSAL)
ul. Sadovaya-Kudrinskaya, d. 9, Moscow, Russia, 125993
izhaev.osman@gmail.com

Valerian A. Lebedev, Dr. Sci. (Law), Professor, Professor, Department of Constitutional and Municipal Law, Kutafin Moscow State Law University (MSAL)
ul. Sadovaya-Kudrinskaya, d. 9, Moscow, Russia, 125993
lebedev_va@bk.ru

Sergey S. Zenin, Cand. Sci. (Law), Associate Professor, Director of the Institute of State and Law, Tyumen State University, Vice-Rector of Tyumen State University; Associate Professor, Department of Constitutional and Municipal Law, Kutafin Moscow State Law University (MSAL)
Volodarsky str., 6, Tyumen, 625003, Russia
zeninsergei@mail.ru

Abstract. The paper analyzes legal approaches to solving key problems of human rights implementation in the conditions of mass exploitation of artificial intelligence (AI) systems in the public space. Within the framework of the study, the emphasis is placed on the features of the legal regulation of the use of artificial intelligence systems for remote biometric identification. The use of these systems is currently only beginning to acquire a regulatory legal framework and law enforcement practice in most countries. The study analyzes several different models of legal regulation that are typical of individual countries and regions, such as the United Kingdom, the United States, China, the EU and Russia.

² The reported study was funded by RFBR according to the research project № 18-29-16193.

In the UK, the use of real-time facial recognition systems in public spaces is allowed, but the set of scenarios and situations of their use is significantly limited by legislation and law enforcement practice. In the United States, both at the federal and state levels, there are no general rules that form a unified legal approach to regulating the area in question. The EC has developed a draft Regulation on Harmonized AI Rules (Artificial Intelligence Act), which is supposed to prohibit the use of AI systems for remote biometric identification of individuals in real time in public places. There is no special regulatory regulation of this sphere of public relations in the PRC. The development of these systems in China is controlled by the state, which, due to the high centralization of power, leads to the risk of human rights violations and the creation of an atmosphere of total surveillance of citizens without any legally established framework and restrictions. In Russia, the state is actively deploying these systems at the federal and regional levels in the absence of a specialized regulatory framework. Human rights are protected only by the general norms of the Constitution of the Russian Federation and legislation, law enforcement practice is mainly aimed at ensuring the interests of the state.

Keywords: face recognition; biometric identification; artificial intelligence; privacy; human rights; intangible benefits.

Cite as: Kuteynikov DL, Izhaev OA, Lebedev VA, Zenin SS. Neprikosновенность частной жизни в условиях использования систем искусственного интеллекта для удаленной биометрической идентификации личности [Privacy in the realm of Artificial Intelligence Systems Application for Remote Biometric Identification]. *Lex russica*. 2022;75(2):121-131. DOI: 10.17803/1729-5920.2022.183.2.121-131. (In Russ., abstract in Eng.).

Введение

Не будет преувеличением сказать, что цифровая среда стала одной из самостоятельных сфер жизнедеятельности общества. Возникающие в этой связи общественные отношения являются сравнительно новыми, и нельзя утверждать, что в правовой науке сформировались устоявшиеся подходы к их регулированию. Напротив, регуляторная политика многих государств находится на стадии поиска наиболее адекватных и эффективных правовых подходов.

На первый взгляд такие традиционные конституционные права, как право на неприкосновенность частной жизни, право на свободу слова и выражения мнений, на информацию и некоторые другие виды прав, полноценно охватывают складывающиеся отношения в сфере информационных технологий. Однако невозможно игнорировать и тот факт, что правовые средства их обеспечения и защиты также должны учитывать особенности данных отношений³.

На уровне государств и частных компаний широко разрабатываются и внедряются в общественное пространство технические средства, основанные на использовании сложных алгоритмов, которые абстрактно в нормативных правовых актах разных стран определяются термином «системы искусственного интеллекта» (ИИ).

Известно, что при осуществлении государственного управления в разных сферах, в том

числе в правоохранительной деятельности, применяются технологии централизованного сбора персональных данных граждан (например, системы цифровых пропусков, позволяющие контролировать передвижения человека, в том числе на транспорте, а также дифференцировать граждан по объему прав; системы видеонаблюдения с технологией распознавания лиц и т.п.). Во многих странах развиваются комплексные государственные системы контроля за общественным пространством. При таких обстоятельствах объем генерируемых данных является беспрецедентным и увеличивается в геометрической прогрессии, вместе с этим увеличиваются и потенциальные риски нарушений прав человека.

Одной из наиболее чувствительных сфер общественной жизни, подвергшихся влиянию практического внедрения технологий, стали отношения, связанные с установлением правовых гарантий защиты прав человека на неприкосновенность частной жизни в связи с применением комплекса технологий систем ИИ для удаленной биометрической идентификации личности. Данные системы, как правило, используются государственными органами в целях обеспечения национальной безопасности (поиск и поимка правонарушителей, предиктивная аналитика совершения правонарушений), однако существуют и иные способы их использования в публичном секторе, например оплата обществен-

³ Livingston S., Risse M. The Future Impact of Artificial Intelligence on Humans and Human Rights // *Ethics & International Affairs*. 2019. No 2. P. 141–158.

ного транспорта, государственных услуг и т.п. Эти системы все чаще находят свое применение и в частном секторе, особенно в сферах банкинга, ритейла, связи, безопасности.

Великобритания: дело R. (Bridges) v. Chief Constable of South Wales Police, 2020

В Великобритании общественность и правозащитные организации выступили широким фронтом против применения полицией систем распознавания лиц в реальном времени в общественных местах после задержания ряда граждан без явных на то оснований⁴.

До недавнего времени использование систем распознавания лиц полицией в Великобритании не имело какой-либо регламентации. В 2019 г. правозащитная организация Liberty обратилась в суд против полиции Южного Уэльса с жалобой на то, что использование полицией системы распознавания лиц в общественных местах нарушает ряд основополагающих нормативных актов, гарантирующих реализацию прав человека, таких как Акт о правах человека, Акт о защите данных и Акт о равенстве⁵. В своем решении суд постановил, что существует достаточная правовая база для обеспечения надлежащего использования системы распознавания лиц в реальном времени и полиция использовала данные системы в полном соответствии с законом⁶.

В 2020 г. Liberty оспорила данное решение суда в апелляционной инстанции (дело R. (Bridges) v. Chief Constable of South Wales Police, 2020). Суд постановил, что использование полицией систем распознавания лиц в реальном времени в отдельных случаях не соответствовало закону. В своем решении суд изложил следующие выводы:

- использование системы распознавания лиц было признано нарушающим право на уважение частной жизни, защищенное Актом о правах человека. Суд обнаружил критические недостатки в правовой базе, оставляющей слишком большую свободу действий для отдельных сотрудников;
- использование системы распознавания лиц нарушает отдельные нормы Акта о защите данных. Основанием является то, что в результате оценки влияния на защиту данных не удалось должным образом оценить риски нарушения прав и свобод субъектов данных, а также не были предусмотрены меры по устранению указанных рисков. Были также определены две группы полномочий, в рамках которых государственные органы обладают недопустимо широкими возможностями для усмотрения: во-первых, каким образом отбираются лица для включения в списки наблюдения, во-вторых, на каком основании в том или ином общественном пространстве размещаются технические комплексы, оснащенные системами распознавания лиц;
- полиция Южного Уэльса нарушила свои обязанности, установленные отдельными положениями Акта о равенстве, так как органы полиции не предприняли попытки как самостоятельно проверить, так и убедиться путем независимой проверки в том, что в работе программного обеспечения отсутствует возможная предвзятость по признаку расы или пола⁷.

На основе данного судебного решения были внесены изменения в Кодекс практики использования камер видеонаблюдения, в соответствии с которыми системные операторы должны основывать свою работу на 12 руководящих принципах, в числе которых ограничение ис-

⁴ UK Government Accused Of Sneaking Through New Live Facial Recognition Rules // URL: <https://www.forbes.com/sites/emmawoolacott/2021/08/23/uk-government-accused-of-sneaking-through-new-live-facial-recognition-rules/?sh=e47cf88706f3> (дата обращения: 01.12.2021).

⁵ B. Gordon Automated Facial Recognition in Law Enforcement: The Queen (On Application of Edward Bridges) v The Chief Constable of South Wales Police // Potchefstroom Electronic Law Journal. 2021. № 24. P. 1–29.

⁶ Independent report Snapshot Paper — Facial Recognition Technology Published 28 May 2020 // URL: <https://www.gov.uk/government/publications/cdei-publishes-briefing-paper-on-facial-recognition-technology/snapshot-paper-facial-recognition-technology#whats-next-for-the-governance-of-frt> (дата обращения: 01.12.2021).

⁷ Briefing note on the ethical issues arising from public-private collaboration in the use of live facial recognition technology (accessible) // URL: <https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf> (дата обращения: 01.12.2021).

черпывающего перечня сфер и сценариев их использования, прозрачность, приоритет прав человека, отсутствие дискриминации по какому-либо признаку⁸.

Таким образом, в Великобритании органами безопасности допускается использование систем распознавания лиц в реальном времени в общественных пространствах, однако набор сценариев и ситуаций их использования существенно ограничен законодательством и правоприменительной практикой. Модель правового регулирования применения указанных систем в данном государстве строится на постоянном диалоге государства и гражданского общества.

США: поиск оптимального баланса

В США на сегодняшний день отсутствует федеральное регулирование использования систем ИИ для биометрической идентификации. Разработка одного или нескольких объемных системообразующих актов неоднократно обсуждалась законодателями, однако пока существует лишь ряд законодательных инициатив, которые находятся на разных стадиях рассмотрения. Во многом это связано с общей политикой правового регулирования систем ИИ и оборота персональных данных этого государства, которые осуществляются *ad hoc*. В 2020 г. принят Указ Президента США и разработаны соответствующие рекомендации для органов исполнительной власти.

Такие технологические компании, как Amazon и Microsoft, ввели мораторий на применение данного комплекса технологий до формирования законодателями достаточной нормативной базы или дорожной карты. Компания IBM, напротив, заявила, что полностью прекратит участие в соответствующих бизнес-проектах⁹.

Разными путями идут законодательство штатов и законодательство отдельных местностей. В ряде штатов и городов использование соответствующего комплекса технологий запрещено полностью или существенно ограничено¹⁰. Применение данных систем привлекло особенно большое внимание общественности после серии митингов Black Lives Matter, а также задержаний после так называемого штурма Капитолия.

Европейский Союз: на заре принятия АИА

В Европейском Союзе разработан проект Регламента ЕС о гармонизированных правилах в отношении ИИ (Artificial Intelligence Act). Данным проектом предполагается установление запрета на использование систем ИИ для удаленной биометрической идентификации физических лиц в режиме реального времени в общедоступных пространствах в целях охраны правопорядка, за исключением трех исчерпывающе перечисленных и узко определенных ситуаций, когда такое использование строго необходимо для достижения существенного общественного интереса, важность которого перевешивает риски.

Данные ситуации включают, во-первых, поиск потенциальных жертв преступлений, включая пропавших детей; во-вторых, угрозу жизни или безопасности человека, в частности при террористических атаках; в-третьих, обнаружение, локализацию, идентификацию и преследование лиц, совершивших или подозреваемых в совершении преступлений по конкретно определенным составам (32 состава уголовных преступлений при сроке лишения свободы не менее 3 лет)¹¹.

Сходную позицию выразили Европейский совет по защите данных (EDPB) и европей-

⁸ Surveillance Camera Code of Practice // URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1010815/Surveillance_Camera_Code_of_Practice__update_.pdf (дата обращения: 01.12.2021).

⁹ Rules around facial recognition and policing remain blurry // URL: <https://www.cnn.com/2021/06/12/a-year-later-tech-companies-calls-to-regulate-facial-recognition-met-with-little-progress.html> (дата обращения: 01.12.2021).

¹⁰ Will there be federal facial recognition regulation in the US? // URL: <https://iapp.org/news/a/u-s-facial-recognition-roundup/> (дата обращения: 01.12.2021).

¹¹ Proposal for a Regulation of the European parliament and of the council laying down harmonised rules on artificial intelligence (Artificial intelligence act) and amending certain union legislative acts com/2021/206 final // URL: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52021PC0206> (дата обращения: 01.12.2021).

ский инспектор по защите данных (EDPS) в отношении ранее опубликованного проекта Регламента Еврокомиссии ЕС о регулировании ИИ. В документе указано, что, принимая во внимание чрезвычайно высокие риски, связанные с удаленной биометрической идентификацией людей в общедоступных местах, EDPB и EDPS призывают к общему запрету на любое использование ИИ для автоматического распознавания человеческих черт в общедоступных местах, в частности распознавание лиц, походки, отпечатков пальцев, ДНК, голоса, нажатия клавиш и других биометрических или поведенческих сигналов, в любом контексте¹².

Таким образом, ЕС близок к формированию устойчивой и многоаспектной системы нормативного правового регулирования использования систем ИИ для удаленной биометрической идентификации личности в реальном времени в общественных местах. При этом регулирование данной сферы общественных отношений в ЕС является «человекоцентричным», что позволяет защищать и гарантировать права и свободы человека, ставя их в центр нормативного обеспечения регулирования в сфере технологического развития. В то же время это несет определенные риски для развития бизнес-процессов, прикладного использования конкретных продуктов в общественном пространстве. Тем не менее ЕС является важным рынком практически для всех крупных технологических компаний и, как и в случае с GDPR, следует ожидать, что такое регулирование, если оно будет принято, станет одним из ключевых подходов, поскольку новые технологические продукты уже будут разрабатываться с учетом имеющихся ограничений.

КНР: от светлого будущего к тотальному контролю

Наиболее широкое применение систем ИИ для удаленной биометрической идентификации личности осуществляется в КНР. Регламентация использования данных систем нашла свое отражение в гражданском законодательстве, а также

в нормативных правовых актах, посвященных кибербезопасности и обороту данных. Какое-либо специальное нормативное регулирование данной сферы общественных отношений к настоящему времени отсутствует. Достаточно большую работу проделала КНР и в сфере защиты данных. В 2016 г. был принят закон о кибербезопасности КНР, который установил сходные с ЕС и США требования к регулированию. Однако в связи с тем, что КНР является государством с авторитарной политической системой, защита конфиденциальности в большей мере связана с решениями органов государственной власти, а не с созданием единого правового поля, поддерживаемого независимыми судебными решениями.

Данная проблема касается и других сфер общественной и экономической деятельности, свобода частных и общественных организаций достаточно жестко ограничена интересами государства. Принимая нормативные правовые акты, государство оставляет за собой массу возможностей по неограниченному участию в деятельности частных компаний, а также активно внедряет инновации для создания единой системы контроля за всеми сферами общественной жизни.

В июле 2017 г. Государственный совет КНР обнародовал стратегию развития ИИ, которая получила название «План развития искусственного интеллекта нового поколения». В данной стратегии перед КНР поставлена цель стать мировым лидером в области ИИ к 2030 г., а также занять лидирующее место в сфере разработки нормативной базы, этических норм и стандартов для ИИ. Сама концепция представляет лишь общую модель и цели будущего правового регулирования, соответственно, ее необходимо рассматривать в комплексе с массой других нормативных правовых актов. Хотя данная концепция и разработана государством, однако фактическая реализация указанных инноваций и преобразований будет осуществляться частным сектором и местными органами власти¹³.

Особенностью нормативного регулирования в КНР также является достаточно быстрая адаптация под использование новых технологиче-

¹² EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination // URL: https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en (дата обращения: 01.12.2021).

¹³ The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation / H. Roberts, J. Cows, J. Morley [et al.] // AI & Soc. 2021. № 36. P. 59–77.

ских решений на широком рынке. Так, в КНР, в отличие от уже рассмотренных стран, активно используются беспилотные автомобили на дорогах общего пользования, на размеченных территориях¹⁴, впервые были созданы автоматизированные интернет-суды, формируется единая система социального рейтинга.

Отличительной чертой КНР является и достаточно высокий по сравнению с другими странами рейтинг одобрения гражданами использования систем видеонаблюдения. Согласно проведенному европейскими учеными исследованию, жители КНР демонстрируют самый высокий уровень согласия на использование технологий распознавания лиц (67 %), а также самое низкое число противников их развертывания (9 %)¹⁵.

Таким образом, с одной стороны, в КНР приняты амбициозные концепции развития в сфере функционирования систем искусственного интеллекта, и инновации значительно активней, чем в ЕС и США, внедряются в общественное пространство за счет централизованного регулирования. С другой стороны, развитие данных систем в КНР подконтрольно государству, что в силу высокой централизации власти приводит к риску нарушения прав человека и созданию атмосферы тотальной слежки за гражданами без каких-либо законодательно установленных рамок и ограничений.

Россия: активное развертывание государственных систем при регуляторном вакууме

В Российской Федерации на данный момент отсутствует специальное регулирование применения данного комплекса технологических решений. Их использование связано общими нормами Конституции РФ, ст. 151.1 и 151.2 ГК РФ, а также Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»¹⁶.

В соответствии с законодательством обработка персональных данных, в том числе биометрических, для установления личности субъекта персональных данных возможна только с письменного согласия последнего, за исключением случаев, представляющих публичный интерес (ч. 2 ст. 11 Федерального закона «О персональных данных»).

Вопрос законности использования систем ИИ для биометрической идентификации личности неоднократно поднимался в судебной практике, однако суды всегда вставали на защиту интересов государства. Например, применение технологии распознавания лиц в г. Москве стало предметом резонансного судебного разбирательства, в результате которого было принято решение Савеловского районного суда от 03.10.2019 об отказе в удовлетворении административного иска в полном объеме, оставленное без изменения апелляционным определением Московского городского суда от 30.01.2020. Истец просила признать незаконными действия ГУ МВД России по г. Москве и Департамента информационных технологий г. Москвы (далее — Департамент) по применению технологии распознавания лиц и обязать их не применять данную технологию, удалить биометрические персональные данные заявителя из базы данных и представить доказательства такого удаления.

Она ссылаясь на то, что в соответствии с ч. 1 ст. 11 Федерального закона «О персональных данных» сведения, характеризующие физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии письменного согласия субъекта персональных данных, за исключением случаев, предусмотренных ч. 2 указанной статьи. В то же время посредством функционирующей при Департаменте городской системы видеонаблюдения с технологией распознавания лиц собираются ее биометрические персональные

¹⁴ Ziyang C., Shiguo L. China's Self-Driving Car Legislation Study // Computer Law and Security Review. 2021. 41. DOI: 10.1016/j.clsr.2021.105555.

¹⁵ Kostka G., Steinacker L., Meckel M. Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States // Public Understanding of Science. 2021. № 30. P. 671–690.

¹⁶ СПС «КонсультантПлюс».

данные, происходит хранение информации о времени и месте ее нахождения без ее согласия. Она полагала, что нарушение ее прав происходит ежедневно, поскольку зарегистрирована и постоянно проживает в г. Москве, посещает публичные места, в которых используются камеры городской системы видеонаблюдения.

Суд отказал в удовлетворении иска в полном объеме, указав на то, что сотрудники ГУ МВД России по г. Москве, которым предоставлен доступ к Единому центру хранения и обработки данных (ЕЦХД), в целях реализации служебных обязанностей используют систему видеоналики на базе ЕЦХД для отождествления лиц, находящихся в федеральном розыске; лиц, которым по решению суда запрещено посещать массовые мероприятия; лиц, находящихся под административным надзором.

Алгоритм распознавания лиц, используемый в ЕЦХД, сравнивает изображение, поступающее в ЕЦХД с видеокамер, с фотографией, предоставленной правоохранительным органом. В процессе обработки соответствующих изображений происходит их сравнение на наличие/отсутствие совпадений. Департаменту не передаются персональные данные (Ф. И. О. и пр.) искомых лиц, поскольку у Департамента нет технической и юридической возможности осуществлять их сопоставление. Таким образом, суд пришел к выводу о том, что при отсутствии процедуры идентификации личности видеоизображения граждан не могут считаться биометрическими персональными данными. Соответственно, отсутствует необходимость получать письменное согласие гражданина на обработку биометрических персональных данных.

Вместе с тем последнее десятилетие российских власти активно занимаются развитием

систем камер с программным обеспечением, использующим системы ИИ для биометрической идентификации личности. По данным доклада «Распознавание лиц: предчувствие антиутопии», подготовленного правозащитными группами «Сетевые свободы» и «Агора», такие системы уже развернуты в 13 регионах¹⁷. Данные разрозненные системы предполагается объединить в единую информационную систему в рамках проекта «Безопасный город»¹⁸.

Таким образом, необходимо дополнительно законодательно урегулировать вопрос относительно процедуры и конкретных случаев использования систем ИИ для удаленной идентификации личности. Активное развертывание государственными органами указанных систем без сформированной на основе широких общественных обсуждений нормативной правовой базы противоречит конституционно установленному принципу правового государства. Представляется, что, несмотря на то, что в ч. 3 ст. 55 Конституции РФ предусмотрена возможность в отдельных случаях ограничения прав и свобод федеральным законом¹⁹, при формулировании конкретной процедуры необходимо избежать умаления прав человека на основе использования принципа пропорциональности. Сам факт введения в эксплуатацию данных систем для обеспечения безопасности не отменяет необходимости соблюдения прав человека.

Авторы рассмотренного выше доклада предлагают ряд минимальных гарантий, направленных на предотвращение возможных злоупотреблений со стороны государственных органов:

«а) обязательное подробное и доступное информирование граждан о применении видеонаблюдения и распознавания лиц;

¹⁷ Гайнутдинов Д., Коротеев К. Распознавание лиц: предчувствие антиутопии : доклад // URL: https://runet.report/static/core/doc/Facial_recognition.pdf (дата обращения: 01.12.2021).

¹⁸ Проект федерального закона «О единой системе обеспечения общественной безопасности, порядка и безопасности среды жизнедеятельности “Безопасный город”»; подготовлен МЧС России, ID проекта 02/04/10-21/00121290; не внесен в ГД ФС РФ, текст по состоянию на 11.10.2021 // URL: <https://regulation.gov.ru/> (дата обращения: 11.10.2021).

¹⁹ По мнению В. Д. Зорькина, «такая общая формулировка таит в себе опасность неоправданно широкого толкования и установления на практике чрезмерных ограничений прав и свобод человека для защиты ценностей общего блага. Особенно если учитывать специфику российского менталитета, связанную с длительными традициями преобладания государственных и общественных интересов над личными интересами» (Зорькин В. Д. Под знаком Основного Закона. Конституционный суд на рубеже четвертого десятилетия // Российская газета. Федеральный выпуск. 2021. № 247 (8598). URL: <https://rg.ru/2021/10/27/konstitucionnyj-sud-na-rubezhe-chetvertogo-desiatiletiia.html> (дата обращения: 01.12.2021)).

- б) перечень разрешенных мест использования и гарантированных “чистых” зон, где видеонаблюдение и FR (распознавание лиц) запрещены;
- в) установление предельного срока хранения с обязательным последующим уничтожением собранных данных;
- г) обязательный независимый аудит;
- д) создание эффективных процедур рассмотрения жалоб на нарушения;
- е) запрет предоставления данных иностранным субъектам, в том числе органам власти»²⁰.

Общественная организация «Роскомсвобода» собирает петиции в рамках кампании по введению моратория на использование технологий распознавания лиц до выработки соответствующей нормативной правовой базы²¹.

Предостережения о преждевременности и об опасности для прав человека использования систем ИИ для дистанционной биометрической идентификации личности неоднократно находили свое отражение в отечественной правовой доктрине²².

Таким образом, однозначно можно утверждать, что использование систем ИИ для дистанционной биометрической идентификации в общедоступных местах способно повлиять на частную жизнь значительной части населения, вызвать ощущение постоянной слежки и косвенно препятствовать осуществлению свободы собраний и других основных прав. Кроме того, вызывает опасение точность функционирования данных систем, а также невозможность исправления допущенных ошибок при использовании данных систем в режиме реального времени.

Необходимо отметить также, что «автоматическое распознавание лиц не просто

отслеживает поведение, но и способно его изменить. Когда подозреваемый знает, что за ним следят, например, во время мирного протеста, его поведение может отличаться от того, каким оно было бы, если бы за ним не следили»²³.

Сведения, собранные государственными органами, должны храниться в защищенных базах данных, подвергаемых аудиту в целях недопущения злоупотреблений, торговли данными, создания каких-либо списков неблагонадежных личностей.

Законодательство большинства демократических стран идет путем создания системы правового регулирования, основанной на подходе, диктующем необходимость соблюдения баланса между защитой прав человека и соблюдением интересов национальной безопасности. Представляется, что отечественному законодательству необходимо на основе принципа пропорциональности урегулировать процедуру и определить конкретные случаи использования систем ИИ для удаленной идентификации личности, не допуская произвольного ограничения прав и свобод человека и гражданина.

Сходную позицию высказал в своей статье В. Д. Зорькин: «Опасность произвольного вторжения законодателя в сферу конституционных прав человека резко возрастает в условиях усиления террористической активности, социально-экономических, экологических кризисов и пандемий. В подобных ситуациях у органов государственной власти возникает большой соблазн пойти по пути ограничения прав граждан в целях защиты прав и законных интересов других лиц, основ конституционного строя, обеспечения безопасности государства и т.д.»²⁴.

²⁰ Гайнутдинов Д., Коротеев К. Указ. соч.

²¹ Кампания против распознавания лиц. Системы распознавания лиц являются технологиями двойного назначения и могут использоваться для давления на общество. Массовое распознавание лиц должно быть запрещено до тех пор, пока не будет обеспечена полная прозрачность и безопасность его использования для граждан // URL: <https://bancam.ru> (дата обращения: 01.12.2021).

²² См.: Технологии распознавания лиц в уголовном судопроизводстве: проблема оснований правового регулирования использования искусственного интеллекта / О. И. Андреева, В. В. Иванов [и др.] // Вестник Томского государственного университета. 2019. № 449. С. 201–212; Букаев Н. М., Исмагилов Р. А. К вопросу соблюдения конституционных прав граждан в уголовном судопроизводстве при использовании в доказывании камер с функцией распознавания лиц // Вестник Уральского юридического института МВД России. 2021. № 1. С. 81–85.

²³ Gordon B. Automated Facial Recognition in Law Enforcement: The Queen (On Application of Edward Bridges) v The Chief Constable of South Wales Police // Potchefstroom Electronic Law Journal. 2021. № 24. P. 1–29.

²⁴ Зорькин В. Д. Указ. соч.

Заключение

В Великобритании за последние годы сложился пласт правового регулирования и правоприменительной практики по использованию систем искусственного интеллекта в общественном пространстве. Органами безопасности допускается использование систем распознавания лиц в реальном времени в общественных пространствах, однако набор сценариев и ситуаций существенно ограничен законодательством и правоприменительной практикой. Модель правового регулирования применения указанных систем в данном государстве строится на постоянном диалоге государства и гражданского общества.

В США на сегодняшний день отсутствует федеральное регулирование использования систем ИИ для биометрической идентификации. Разными путями идут законодательство штатов и законодательство отдельных местностей. В ряде штатов и городов применение соответствующего комплекса технологий запрещено полностью или существенно ограничено.

В Евросоюзе разработан проект Регламента ЕС о гармонизированных правилах в отношении ИИ (Artificial Intelligence Act). Данным проектом предполагается установление запрета на использование систем ИИ для удаленной биометрической идентификации физических лиц в

режиме реального времени в общедоступных пространствах в целях охраны правопорядка, за исключением трех исчерпывающе перечисленных и узко определенных ситуаций, когда такое использование строго необходимо для достижения существенного общественного интереса, важность которого перевешивает риски.

В КНР отсутствует специальное нормативное регулирование данной сферы общественных отношений. Регламентация использования систем ИИ нашла свое отражение в гражданском законодательстве, а также в нормативных правовых актах, посвященных кибербезопасности и обороту данных. Развитие этих систем в КНР подконтрольно государству, что в силу высокой централизации власти приводит к риску нарушения прав человека и создания атмосферы тотальной слежки за гражданами без каких-либо законодательно установленных рамок и ограничений.

В России государство активно разворачивает данные системы на региональном и федеральном уровнях при отсутствии какой-либо специализированной нормативной правовой базы. Права человека защищены лишь общими нормами Конституции и других законов, сложившаяся правоприменительная практика направлена преимущественно на обеспечение интересов государства.

БИБЛИОГРАФИЯ

1. Андреева О. И., Иванов В. В., Нестеров А. Ю., Трубникова Т. В. Технологии распознавания лиц в уголовном судопроизводстве: проблема оснований правового регулирования использования искусственного интеллекта // Вестник Томского государственного университета. — 2019. — № 449. — С. 201–212.
2. Букаев Н. М., Исмагилов Р. А. К вопросу соблюдения конституционных прав граждан в уголовном судопроизводстве при использовании в доказывании камер с функцией распознавания лиц // Вестник Уральского юридического института МВД России. — 2021. — № 1. — С. 81–85.
3. Зорькин В. Д. Под знаком Основного Закона. Конституционный суд на рубеже четвертого десятилетия // Российская газета. Федеральный выпуск. 2021. № 247 (8598). URL: <https://rg.ru/2021/10/27/konstitucionnyj-sud-na-rubezhe-chetvertogo-desiatiletiia.html> (дата обращения: 01.12.2021).
4. Gordon B. Automated Facial Recognition in Law Enforcement: The Queen (On Application of Edward Bridges) v The Chief Constable of South Wales Police // Potchefstroom Electronic Law Journal. — 2021. — № 24. — P. 1–29.
5. Kostka G., Steinacker L., Meckel M. Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States // Public Understanding of Science. — 2021. — № 30. — P. 671–690.
6. Livingston S., Risse M. The Future Impact of Artificial Intelligence on Humans and Human Rights // Ethics & International Affairs. — 2019. — No 2. — P. 141–158.
7. Roberts H., Cows J., Morley J. et al. The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation // AI & Soc. — 2021. — № 36. — P. 59–77.
8. Ziyang C., Shiguo L. China's Self-Driving Car Legislation Study // Computer Law and Security Abstract. — 2021. — 41. — DOI:10.1016/j.clsr.2021.105555.

Материал поступил в редакцию 10 января 2022 г.

REFERENCES

1. Andreeva OI, Ivanov VV, Nesterov AYU, Trubnikova TV. Tekhnologii raspoznavaniya lits v ugovnom sudoproizvodstve: problema osnovaniy pravovogo regulirovaniya ispolzovaniya iskusstvennogo intellekta [Facial recognition technologies in criminal proceedings: the problem of the grounds for legal regulation of the use of artificial intelligence]. *Vestnik Tomskogo gosudarstvennogo universiteta [Tomsk State University Journal]*. 2019;449:201-212. (In Russ.)
2. Bukaev NM, Ismagilov RA. K voprosu soblyudeniya konstitutsionnykh prav grazhdan v ugovnom sudoproizvodstve pri ispolzovanii v dokazyvanii kamer s funktsiey raspoznavaniya lits [On the issue of compliance with the constitutional rights of citizens in criminal proceedings when using cameras with face recognition function]. *Vestnik Uralskogo yuridicheskogo instituta MVD Rossii*. 2021;1:81-85. (In Russ.)
3. Zorkin VD. Potentsial obnovennoy Konstitutsii [The potential of the updated Constitution]. *Rossiyskaya gazeta. Federalnyy vypusk*. No. 247 (8598). 2021 October 27. Available from: <https://rg.ru/2021/10/27/konstitucionnyj-sud-na-rubezhe-chetvertogo-desiatiletiia.html> [cited 2021 December 01]. (In Russ.)
4. Gordon B. Automated Facial Recognition in Law Enforcement: The Queen (On Application of Edward Bridges) v The Chief Constable of South Wales Police. *Potchefstroom Electronic Law Journal*. 2021;24:1-29.
5. Kostka G, Steinacker L, Meckel M. Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States. *Public Understanding of Science*. 2021;30:671-690.
6. Livingston S, Risse M. The Future Impact of Artificial Intelligence on Humans and Human Rights. *Ethics & International Affairs*. 2019;2:141-158.
7. Roberts H, Cowls J, Morley J, et al. The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation. *AI & Soc*. 2021;36:59-77.
8. Ziyang C, Shiguo L. China's Self-Driving Car Legislation Study. *Computer Law and Security Abstract*. 2021;41. DOI:10.1016/j.clsr.2021.105555.