

## ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ БИОМЕТРИЧЕСКИХ ТЕХНОЛОГИЙ В МУНИЦИПАЛЬНЫХ ОБРАЗОВАНИЯХ\*

**А.Ю. Чурикова<sup>1,2</sup>, М.А. Липчанская<sup>3,4</sup>**

<sup>1</sup> Саратовская государственная юридическая академия, г. Саратов, Россия

<sup>2</sup> Государственный университет управления, г. Москва, Россия

<sup>3</sup> Российский государственный университет правосудия, г. Москва, Россия

<sup>4</sup> Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, г. Москва, Россия

### **Информация о статье**

Дата поступления –

16 ноября 2024 г.

Дата принятия в печать –

20 июня 2025 г.

Дата онлайн-размещения –

20 сентября 2025 г.

Рассмотрен российский и европейский подходы к регулированию технологий, использующих биометрические персональные данные. Выделены и проанализированы три ключевых направления применения биометрических технологий муниципальными органами власти: обеспечение безопасности; оказание муниципальных услуг; анализ данных и планирование. Выявлены проблемы правоприменения, связанные с несовершенством действующего законодательства, и предложены пути их устранения.

### **Ключевые слова**

Местное самоуправление,  
цифровая трансформация,  
искусственный интеллект,  
биометрическая  
аутентификация,  
биометрическая  
идентификация,  
биометрические персональные  
данные

## PROBLEMS OF USING BIOMETRIC TECHNOLOGIES IN MUNICIPALITIES\*\*

**Anna Yu. Churikova<sup>1,2</sup>, Maria A. Lipchanskaya<sup>3,4</sup>**

<sup>1</sup> Saratov State Law Academy, Saratov, Russia

<sup>2</sup> State University of Management, Moscow, Russia

<sup>3</sup> Russian State University of Justice, Moscow, Russia

<sup>4</sup> Russian Presidential Academy of National Economy and Public Administration, Moscow, Russia

### **Article info**

Received –

2024 November 16

Accepted –

2025 June 20

Subject. The article analyzes issues related to the regulation and use of biometric technologies and biometric data. The choice of the object of the study is due to the intensive development and implementation of technologies based on the fact that biometric personal data are actively moving and used not only to provide power, but also in private organizations. At the municipal level, the problems of legal regulation and law enforcement are especially acute.

\* Исследование выполнено за счет гранта Российского научного фонда № 23-28-01252, <https://rscf.ru/project/23-28-01252/> «Трансформация института местного самоуправления в Российской Федерации в условиях развития современных цифровых технологий: правовые аспекты», финансирование осуществляется через ФГБОУ ВО «Государственный университет управления».

\*\* The research was carried out at the expense of the grant of the Russian Science Foundation No. 23-28-01252, <https://rscf.ru/project/23-28-01252/>, “Transformation of the institution of local self-government in the Russian Federation in the context of the development of modern digital technologies: legal aspects”, financing is carried out through the organization of State University of Management.

Available online –  
2025 September 20

**Keywords**

Local government, digital transformation, artificial intelligence, biometric authentication, biometric identification, biometric personal data

The purpose of the study: based on the analysis of law enforcement practice and consideration of different approaches to regulating the use of biometric technologies, formulate specific proposals for improving the legal regulation of the use of biometric digital data when using face measurement technologies.

Methodology. The methodological substantiation of the study was a set of methods of cognition, the methods of which were: monitoring of law enforcement practice, comparative legal method, analysis method, systemic-structural method.

Conclusions. Based on the results of the study, the following conclusions were made:

(1) Municipal biometric technologies are used to provide food for the purpose of: ensuring labor safety on the territory of the municipality; biometric identification and authentication, including when providing municipal services; data analysis and planning.

(2) The conditions for limiting the rights and freedoms of an individual when using biometric technologies depend on the level of use of these technologies, as well as on the degree of regulatory regulation of their application. In conditions where the norms and rules are legally observed, the risks of negative consequences as a result of the use of data transmission technologies are the lowest. Blanket norms establishing exceptions for the use of biometric data have a negative impact on law enforcement practice.

(3) Excessively strict restrictions, as well as a ban on the use of municipal government organizations and commercial organizations, technologies, actors in real time, do not allow for the organization of an effective public safety system, and therefore it is necessary to establish balanced legal regulation. The harmonization of this area will be facilitated by introducing amendments to the current legislation proposed by the authors of the article, aimed at, on the one hand, protecting the rights of an individual when using face and emotion technologies in public places, and, on the other hand, ensuring the possibility of using data technologies for the purpose of creating a modern level of security for the population in the territory of a municipality.

**1. Введение**

Биометрические технологии идентификации и аутентификации личности, в том числе используемые в режиме реального времени, всё более активно применяются муниципальными органами власти. Данные технологии могут использоваться для мониторинга общественных мест и быстрого реагирования на потенциальные угрозы, что позволяет своевременно предотвращать правонарушения и обеспечивать общественный порядок [1, с. 123–125]. В связи с этим М.С. Абламейко и Р.П. Богущ указывают, что «системы интеллектуального видеонаблюдения сегодня стали неотъемлемой частью “умных городов”» [2, с. 15].

Создание систем интеллектуального видеонаблюдения дворовых территорий и объектов муниципальной инфраструктуры является одним из направлений цифровой трансформации местного самоуправления как в России, так и за рубежом [3, с. 223–225; 4; 5, р. 152–154]. Однако применение биометрических технологий, особенно в общественных местах, поднимает ряд этических и правовых вопросов о допустимости и пределах вмешательства в частную жизнь граждан [6, р. 167–169; 7, р. 121–125; 8, р. 658–660]. С началом эксплуатации технологий распозна-

вания лиц возник комплекс проблем, связанных с конфиденциальностью, защитой биометрических персональных данных (далее – БПД), отсутствием правовой определенности в разрешении вопросов о возможностях и пределах использования БПД муниципальными органами власти, частными лицами и правоохранительными органами [9, с. 19–20; 10, с. 80–81; 11; 12, с. 828–831; 13, с. 111–114].

Комплекс неразрешенных правовых и фактических проблем, связанных с эксплуатацией биометрических технологий, а также потребность в разработке правовой базы, регулирующей использование таких технологий органами местного самоуправления, обуславливают высокую степень актуальности данной темы.

В связи с этим цель настоящего исследования заключается в формулировании конкретных предложений по совершенствованию действующего законодательства на основе анализа правоприменительной практики и рассмотрения разных подходов к регулированию эксплуатации биометрических технологий.

**2. Методология исследования**

При проведении исследования осуществлялся мониторинг правоприменительной практики. Проводился поиск судебных решений, содержащих упо-

минание применения технологии распознавания лиц, а также системы интеллектуального видеонаблюдения, что позволило выявить существующие в практической деятельности проблемы эксплуатации биометрических технологий. Использование сравнительно-правового метода позволило рассмотреть различные подходы к регулированию эксплуатации биометрических технологий. Междисциплинарный подход, а также применение метода анализа способствовали комплексности проведенного исследования и обеспечили разностороннее рассмотрение заявленной темы. Для обеспечения последовательного исследования проблем правоприменения, возникающих при эксплуатации технологии распознавания лиц местными органами власти, использовался системно-структурный метод.

### 3. Компаративистский анализ правового регулирования использования органами местного самоуправления биометрической идентификации и аутентификации

Технологии распознавания лиц и эмоций на основе БПД, также именуемые биометрическими технологиями [14, с. 90] либо технологиями биометрической идентификации [15, с. 33], являются разновидностями технологий искусственного интеллекта (далее также – ИИ) [16, с. 55–59; 17, р. 407; 18], которые регламентом Европейского Парламента и Совета 2024 г. (далее – Закон ЕС об ИИ) отнесены к категории неприемлемого риска<sup>1</sup>.

Такая оценка данных технологий в Европейском Союзе обусловлена высокой вероятностью ограничения прав и свобод человека и гражданина при их эксплуатации. Закон ЕС об ИИ содержит ограничения и перечень случаев, когда БПД могут быть использованы для удаленной биометрической идентификации и категоризации в целях обеспечения соблюдения закона. В России подобных ограничений на эксплуатацию биометрических технологий не установлено, но действует ограничение на применение БПД, закрепленное в ст. 11 Федерального закона от

27 июля 2006 г. № 152-ФЗ (далее – Закон о персональных данных)<sup>2</sup>, при этом используется достаточно широкий субъективный подход к определению того, какая информация является БПД [19, с. 80, 86].

Биометрические технологии могут использоваться органами местного самоуправления в разных направлениях и с различными целями, что будет определять степень их воздействия на права и законные интересы личности. То есть *риск представляют не сами технологии распознавания лиц и эмоций, а совокупность их характеристик и направленный эксплуатационный*.

Одно из наиболее распространенных оснований применения данных технологий – это обеспечение правопорядка. Посредством систем интеллектуального видеонаблюдения возможно проведение биометрической идентификации личности в режиме реального времени [20, р. 293–295; 21, р. 586–588]. Таким способом осуществляется поиск правонарушителей и установление их личности (актуально при осуществлении муниципального контроля).

Понятия биометрической аутентификации и идентификации закреплены и в Законе ЕС об ИИ, и в Федеральном законе от 29 декабря 2022 г. № 572-ФЗ (далее – Закон об идентификации и аутентификации)<sup>3</sup>.

Согласно Закону ЕС об ИИ биометрическая идентификация – это автоматизированное распознавание физических, физиологических и поведенческих черт человека, таких как лицо, движение глаз, форма тела, голос, просодия, походка, осанка, частота сердечных сокращений, артериальное давление, запах, характеристики нажатия клавиш, с целью установления личности человека путем сравнения биометрических данных этого человека с сохраненными биометрическими данными людей в справочной базе данных, независимо от того, дал ли человек свое согласие или нет. Данное определение исключает биометрическую аутентификацию, целью которой является подтверждение личности физического

<sup>1</sup> См.: European Parliament legislative resolution of 13 March 2024 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts (COM(2021)0206; C9-0146/2021; 2021/0106(COD)). URL: [https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138\\_EN.html#title1](https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.html#title1) (дата обращения: 27.08.2024).

<sup>2</sup> См.: Федеральный закон от 27 июля 2006 г. № 152-ФЗ (с изм. и доп. от 8 августа 2024 г., № 233-ФЗ) «О персональных данных» // Собрание законодательства Российской

Федерации. 2006. № 31 (ч. I). Ст. 3451; 2024. № 33 (ч. I). Ст. 4929.

<sup>3</sup> См.: Федеральный закон от 29 декабря 2022 г. № 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» // Собрание законодательства Российской Федерации. 2023. № 1 (ч. I). Ст. 19.

лица для получения доступа к услуге либо разблокировки устройства или обеспечения безопасного доступа в помещения. Разделение этих понятий объективно обусловлено разницей категорий риска эксплуатации одной и той же технологии для разных целей.

Согласно Закону ЕС об ИИ использование технологии распознавания лиц для повышения уровня безопасности на территории муниципалитетов ограничено случаями поиска подозреваемых, осужденных, без вести пропавших лиц, установления личности в случае невозможности получить сведения от самого лица.

Использование биометрических технологий в совокупности с технологией анализа больших данных позволяют качественно улучшить подход к решению управленческих задач на муниципальном уровне. Например, системы видеонаблюдения с функцией распознавания лиц могут использоваться для сбора статистических данных о посещаемости различных объектов и мероприятий, что может помочь в их планировании и организации. Также некоторые авторы предлагают использовать технологии распознавания лиц для оптимизации и индивидуализации туристических предложений [22, р. 1179–1180].

Согласно ст. 9 Закона об идентификации и аутентификации органы местного самоуправления могут осуществлять идентификацию по БПД, используя уникальное обозначение сведений о лице, необходимое для определения такого лица только через Единую систему идентификации и аутентификации физических лиц с использованием биометрических персональных данных (ЕСИА), при этом результатом идентификации является установление сведений о лице, а аутентификации – установление лица<sup>4</sup>.

С.С. Кузнецова, А.Н. Мочалов и М.С. Саликов, анализируя сложившиеся в России и в некоторых зарубежных странах модели правового регулирования биометрической идентификации, отмечают, что отечественное регулирование «в большей степени тяготеет к модели, выбранной Китаем» [23, с. 263], т. е. публичные интересы преобладают над частными. Подобный подход имеет как положительные, так и

негативные стороны. Так, Ш. Цзя и Ц. Чжан указывают, что проблемы в китайском правовом регулировании применения технологии распознавания лиц приводят к утечке и несанкционированному использованию БПД [24, с. 276–279].

В России *перечень исключений по использованию БПД, закрепленный в Законе о персональных данных, носит отсылочный, неконкретизированный характер*. При буквальном толковании закона возможности муниципальным органам власти или частным лицам использовать БПД без письменного согласия субъекта персональных данных для обеспечения правопорядка либо для оказания услуг, в том числе муниципальных, не предоставляется, но на практике БПД и соответствующие технологии повсеместно используются.

#### 4. Практические аспекты эксплуатации биометрических технологий при идентификации и аутентификации

Несмотря на правовые сложности применения биометрических технологий, они активно применяются для идентификации личности и органами власти, и хозяйствующими субъектами, что дает возможность формирования единой системы, способствующей обеспечению безопасности населения на определенной территории. Так, согласно Приказу Комитета правопорядка и безопасности Ленинградской области от 8 мая 2024 г. № 12 средства и системы видеонаблюдения, принадлежащие органам местного самоуправления, муниципальным учреждениям и предприятиям, хозяйствующим субъектам, осуществляющим деятельность на территории Ленинградской области, включаются в систему интеллектуального видеонаблюдения и видеоаналитики «Безопасный город» на территории Ленинградской области<sup>5</sup>.

Камеры интеллектуального видеонаблюдения с возможностью распознавания лиц находятся в свободной продаже и используются многими коммерческими организациями и частными лицами, что делает эту технологию доступной для применения не только государственными и муниципальными органами власти. Нередко системы распознавания лиц

<sup>4</sup> См.: Письмо Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 28 декабря 2023 г. № П24-2-04-070-257558 «О направлении информации» // СПС «КонсультантПлюс».

<sup>5</sup> Приказ Комитета правопорядка и безопасности Ленинградской области от 8 мая 2024 г. № 12 «Об утверждении требований к локальным системам видеонаблюдения и к

дополнительным технологическим каналам передачи данных, включаемым в систему интеллектуального видеонаблюдения и видеоаналитики аппаратно-программного комплекса «Безопасный город» на территории Ленинградской области». URL: <https://npa.lenobl.ru/docs/government/view/108656/> (дата обращения: 19.08.2024).

позволяют не только устанавливать личность, но и выявлять преступления. Например, по делу № 1-367/2023 установить факт хищения денежных средств и задержать лицо, совершившее данное преступное деяние, удалось благодаря системе распознавания лиц. Директор магазина через приложение «Контроль распознавания лиц» получила уведомление о распознавании в служебном кабинете неизвестного мужчины, что позволило своевременно подойти к помещению и не дать скрыться лицу, проникшему в него<sup>6</sup>. В данном случае произошло распознавание лица, чьи биометрические данные не были внесены в систему. Однако нередко в судебной практике встречаются случаи внесения БПД лиц без их на то согласия представителями коммерческих организаций в соответствующую систему. Например, сотрудник магазина, просмотрев записи с камер видеонаблюдения, установленных в магазине, обнаружил, что в магазин зашел мужчина, взял товар и покинул магазин без оплаты товара. Сотрудник магазина внес изображение лица мужчины, похитившего товар, в систему распознавания лиц, установленную в сети данных магазинов. В этот же день ему на телефон пришло сообщение от системы распознавания лиц, что мужчина, БПД которого были внесены в систему, находится в магазине. Охрана магазина задержала данного мужчину, несмотря на то, что в этот раз он ничего не похищал<sup>7</sup>.

Если расценивать все эксплуатируемые коммерческими организациями на территории муниципального образования системы распознавания лиц как составную часть системы обеспечения безопасности на территории муниципального образования, то, безусловно, в таком использовании биометрических технологий есть определенные плюсы. Однако вопросы, связанные с применением технологий распознавания лиц коммерческими организациями в ситуациях, подобных рассмотренным, не урегулированы. Требуется принятие мер для предотвращения рисков недобросовестного использования биометрических технологий. Также представляется необходимым информирование муниципальных органов власти о применении подобных технологий коммерческими организациями на территории муниципаль-

ного образования, что способствовало бы выстраиванию органами местного самоуправления системы обеспечения безопасности населения на территории муниципального образования.

Использование биометрической идентификации и аутентификации лиц при предоставлении муниципальных услуг также является важным направлением применения биометрических технологий, способным упростить доступ к оказываемым услугам и, в то же время, обеспечить надежную идентификацию личности. В судебной практике рассмотрение жалоб, поступивших в электронном виде без прохождения соответствующей идентификации, аутентификации, при отсутствии электронной подписи, признаётся незаконным, даже если эти обращения поступали через официальные сервисы государственных и муниципальных органов власти. Например, решение заместителя начальника Государственной административно-технической инспекции признано судом незаконным, так как жалоба, по которой было принято данное решение, поступила через сервис электронных обращений в инспекцию, а не через портал госуслуг, она не была подписана электронной подписью, а у заявителя отсутствовало «наличие подтвержденной ЕСИА»<sup>8</sup>.

Представляется, что требование об обязательной идентификации и аутентификации не должно ограничивать возможности граждан и организаций по взаимодействию с муниципальными органами власти в цифровом формате. Правила такого взаимодействия должны разъясняться. При этом, если требуется подача определенных видов жалоб или обращений с прохождением идентификации и аутентификации именно через сайт государственных и муниципальных услуг, то должно быть обеспечено перенаправление пользователей при попытке подать данные жалобы или обращения через иные сервисы государственных или муниципальных органов власти.

Проблемы возникают также при поставке оборудования и программного обеспечения. Так, по делу № 22-2544/2023 органами следствия директор муниципального казенного учреждения (оправдан в связи с отсутствием в его действиях состава преступления) обвинялся в том, что не принял мер к органи-

<sup>6</sup> Приговор № 1-367/2023 от 21 августа 2023 г. URL: <https://судебныерешения.рф/77750071> (дата обращения: 18.07.2024).

<sup>7</sup> Приговор № 1-975/2023 от 12 октября 2023 г. URL: <https://судебныерешения.рф/78098889> (дата обращения: 19.07.2024).

<sup>8</sup> Решение № 12-564/2024 от 15 июля 2024 г. URL: <https://судебныерешения.рф/83504537> (дата обращения: 18.08.2024).

зации надлежащего контроля за сверкой качественных характеристик камер видеонаблюдения, поставленных в рамках муниципального контракта на оказание услуг по созданию системы интеллектуального видеонаблюдения дворовых территорий. Из показаний инженера, допрошенного в качестве свидетеля, следует, что при выполнении работ возникли сложности с настройкой камер, связанные со сбоями в распознавании лиц, кроме того, после замены камер, без прошивки и написания софт-программ, новые камеры не выполняли бы свои функции<sup>9</sup>. Это свидетельствует о практической значимости создания оборудования и разработки качественного отечественного программного обеспечения, позволяющих применять биометрические технологии. В связи с чем считаем обоснованным предложение К.А. Пономаревой о необходимости закрепления мер поддержки ИТ-компаний в национальном законодательстве, а также о том, что требуется «предусмотреть специальные правила исчисления и уплаты налога на прибыль иностранных цифровых компаний и параллельно расширять меры налогового стимулирования российских компаний» [25, с. 618].

#### **5. Предложения по решению выявленных проблем правового регулирования и правоприменения**

Для обеспечения возможности использования технологии распознавания лиц муниципальными органами власти для целей обеспечения безопасности и правопорядка на территории муниципального образования, а также в целях защиты прав и свобод человека и гражданина при использовании данной технологии в общественных местах предлагаем внести следующие изменения в действующее законодательство:

1) дополнить ст. 11 Закона о персональных данных ч. 1.1 следующего содержания: «В местах использования технологий, позволяющих установить личность по биометрическим персональным данным, осуществляется обязательное информирование о применении данной технологии посредством размещения опознавательных знаков»;

2) дополнить ч. 2 ст. 11 Закона о персональных данных следующим предложением: «Биометрические персональные данные могут быть внесены в систему распознавания лиц без добровольного информированного согласия лица при наличии фактиче-

ских документированных оснований, включая фото-, видео- и аудиоданные, позволяющих подозревать противоправное поведение лица. Уведомление о внесении биометрических персональных данных в систему распознавания лиц без согласия субъекта персональных данных, а также причины внесения такой информации в течение суток должно быть направлено в уполномоченный орган по защите прав субъектов персональных данных».

Также необходимым представляется обязательное формирование перечня организаций, использующих биометрические технологии, на территории муниципального образования, что будет способствовать быстрому и эффективному взаимодействию органов местного самоуправления, правоохранительных органов и представителей хозяйствующих субъектов.

#### **6. Заключение**

Проведенное исследование позволяет сделать следующие основные выводы и предложения:

1. В Европейском Союзе устанавливаются существенные ограничения на использование биометрических технологий в тех случаях, когда их применение препятствует реализации права на тайну частной жизни лица, а также других гарантированных законом прав и свобод. В России ограничивается применение не самих технологий, а использование БПД, что также приводит к сужению перечня возможностей эксплуатации соответствующих технологий.

2. Муниципальными органами власти биометрические технологии могут применяться с целью обеспечения безопасности населения на территории муниципального образования; прохождения биометрической идентификации и аутентификации, в том числе при оказании муниципальных услуг; анализа данных и планирования.

3. Вероятность ограничения прав и свобод личности при эксплуатации биометрических технологий зависит от направлений использования данных технологий, а также от степени нормативной урегулированности их применения. В условиях отсутствия законодательно установленных норм и правил возникают наибольшие риски негативных последствий от произвольного применения данных технологий. Бланкетный характер норм, устанавливающих исключения для использования БПД, оказывает негативное воздействие на правоприменительную практику.

<sup>9</sup> Апелляционное постановление № 22-2544/2023 от 31 августа 2023 г. URL: <https://судебныерешения.рф/77689566> (дата обращения: 15.08.2024).

4. Излишне жесткие ограничения, а также запрет на применение муниципальными органами власти и коммерческими организациями технологий распознавания лиц в режиме реального времени не позволит обеспечить организацию эффективной системы общественной безопасности, в связи с чем необходимо установление сбалансированного правового регулирования. Способствовать гармонизации данной сферы будет принятие предлагаемых ав-

торами статьи изменений в действующее законодательство, направленных, с одной стороны, на защиту прав личности при использовании технологий распознавания лиц и эмоций в общественных местах, а с другой, – на обеспечение возможности эксплуатации данных технологий с целью создания высокого уровня безопасности для населения на территории муниципального образования.

### СПИСОК ЛИТЕРАТУРЫ

1. Кутейников Д. Л. Неприкосновенность частной жизни в условиях использования систем искусственного интеллекта для удаленной биометрической идентификации личности / Д. Л. Кутейников, О. А. Ижаев, Л. В. Алексеевич, С. С. Зенин // *Lex russica*. – 2022. – Т. 75, № 2. – С. 121–131. – DOI: 10.17803/1729-5920.2022.183.2.121-131.
2. Абламейко М. С. Интеллектуальное видеонаблюдение в «умном городе»: контроль и защита визуальных персональных данных / М. С. Абламейко, Р. П. Богуш // *Судебная экспертиза Беларуси*. – 2023. – № 1 (16). – С. 15–23.
3. Можаяева С. Ю. О некоторых вопросах использования биометрической идентификации в целях выявления преступлений и правонарушений поднадзорных лиц / С. Ю. Можаяева, С. А. Можаяев // *Вестник Воронежского института МВД России*. – 2024. – № 2. – С. 223–227.
4. Bibri S. E. A Novel Model for Data-Driven Smart Sustainable Cities of the Future: A Strategic Roadmap to Transformational Change in the Era of Big Data / S. E. Bibri, J. Krogstie // *Future Cities and Environment*. – 2021. – Vol. 7. – Art. 3. – DOI: 10.5334/fce.116.
5. Benkő M. Real vs. Virtual City: Planning Issues in a Discontinuous Urban Area in Budapest's Inner City / M. Benkő, B. Bene, Á. Pírity, Á. Szabó, T. Egedy // *Urban Planning*. – 2021. – Vol. 6, No. 4. – P. 150–163. – DOI: 10.17645/up.v6i4.4446.
6. Smith M. The ethical application of biometric facial recognition technology / M. Smith, S. Miller // *AI & Society*. – 2022. – Vol. 37, Iss. 1. – P. 167–175. – DOI: 10.1007/s00146-021-01199-9.
7. Mann M. Automated facial recognition technology: Recent developments and approaches to oversight / M. Mann, M. Smith // *University of New South Wales Law Journal*. – 2017. – Vol. 40, Iss. 1. – P. 121–145. – DOI: 10.53637/KAVV4291.
8. Kavoliūnaitė-Ragauskienė E. Right to Privacy and Data Protection Concerns Raised by the Development and Usage of Face Recognition Technologies in the European Union / E. Kavoliūnaitė-Ragauskienė // *Journal of Human Rights Practice*. – 2024. – Vol. 16, Iss. 2. – P. 658–674. – DOI: 10.1093/jhuman/huad065.
9. Бабаева Ю. Г. Биометрический образ: правовое регулирование цифровых данных о человеке / Ю. Г. Бабаева, В. Б. Израелян // *Вестник Университета Правительства Москвы*. – 2022. – № 3 (57). – С. 17–23.
10. Затолокин А. А. Административно-правовые аспекты государственного регулирования обработки биометрических персональных данных / А. А. Затолокин, В. В. Стрельцов // *Общество и право*. – 2023. – № 1 (83). – С. 79–83.
11. Pereira R. S. Remarks on the Use of Biometric Data Systems (and Facial Recognition Technologies) for Law Enforcement Purposes: Security Implications of the Proposal for an EU Regulation on Artificial Intelligence / R. S. Pereira // *The Legal Challenges of the Fourth Industrial Revolution. The European Union's Digital Strategy* / eds. D. Moura Vicente, S. de Vasconcelos Casimiro, C. Chen. – Cham, Springer, 2023. – P. 193–209. – (Law, Governance and Technology Series; vol. 57). – DOI: 10.1007/978-3-031-40516-7\_11.
12. Утеген Д. Технология распознавания лиц и обеспечение безопасности биометрических данных: сравнительный анализ моделей правового регулирования / Д. Утеген, Б. Ж. Рахметов // *Journal of Digital Technologies and Law*. – 2023. – Т. 1, № 3. – С. 825–844. – DOI: 10.21202/jdtl.2023.36.
13. Ковалева Н. Н. Проблемы обеспечения конфиденциальности персональных данных при использовании систем искусственного интеллекта / Н. Н. Ковалева, Н. А. Жирнова // *Журнал российского права*. – 2024. – Т. 28, № 7. – С. 109–121. – DOI: 10.61205/S160565900027561-1.

14. Рывкин С. Ю. Биометрические технологии – новый уровень идентификации человека / С. Ю. Рывкин, В. А. Галкина // *Моя профессиональная карьера*. – 2019. – № 7, т. 4, – С. 90–95.
15. Афанасьев С. Д. Биометрическая идентификация и права человека: демаркационная линия / С. Д. Афанасьев, И. А. Терещенко, Д. А. Яцкевич // *Закон*. – 2022. – № 3. – С. 33–46. – DOI: 10.37239/0869-4400-2022-18-3-33-46.
16. Колоденкова А. Е. Онтология идентификации человека по движениям тела и лицу в видеонаблюдениях / А. Е. Колоденкова // *Онтология проектирования*. – 2023. – Т. 13, № 1. – С. 55–74. – DOI: 10.18287/2223-9537-2023-13-1-55-74.
17. Mishchenko E. Y. Model of Identification of a Person in Databases of Various Sizes / E. Y. Mishchenko, A. N. Sokolov // *2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBREIT)*. – IEEE, 2021. – P. 407–410. – DOI: 10.1109/USBREIT51232.2021.9455020.
18. Иванов В. А. Реальная вероятность распознавания изображений лиц людей с использованием искусственных нейронных сетей / В. А. Иванов, А. А. Смирнов, Д. А. Николаев // *Радиотехника*. – 2022. – Т. 86, № 1. – С. 55–60. – DOI: 10.18127/j00338486-202201-09.
19. Кривогин М. С. Особенности правового регулирования биометрических персональных данных / М. С. Кривогин // *Право. Журнал Высшей школы экономики*. – 2017. – № 2. – С. 80–89.
20. Jaiswal A. Real-Time Biometric System for Security and Surveillance Using Face Recognition / A. Jaiswal, S. Tarar // *Advances in Computing and Data Sciences : 4th International Conference, ICACDS 2020, Valletta, Malta, April 24–25, 2020 : Revised Selected Papers* / eds. M. Singh, P. Gupta, V. Tyagi, J. Flusser, T. Ören, G. Valentino. – Singapore : Springer, 2020. – P. 293–304. – (Communications in Computer and Information Science; vol. 1244). – DOI: 10.1007/978-981-15-6634-9\_27.
21. Fabrègue B. F. G. Privacy and Security Concerns in the Smart City / B. F. G. Fabrègue, A. Bogoni // *Smart Cities*. – 2023. – Vol. 6, Iss. 1. – P. 586–613. – DOI: 10.3390/smartcities6010027.
22. Gupta S. The future is yesterday: Use of AI-driven facial recognition to enhance value in the travel and tourism industry / S. Gupta, S. Modgil, C. K. Lee, U. Sivarajah // *Information Systems Frontiers*. – 2023. – Vol. 25, Iss. 3. – P. 1179–1195. – DOI: 10.1007/s10796-022-10271-8.
23. Кузнецова С. С. Биометрическая идентификация в Интернете: тенденции правового регулирования в России и за рубежом / С. С. Кузнецова, А. Н. Мочалов, М. С. Саликов // *Вестник Томского государственного университета*. – 2022. – № 476. – С. 257–267. – DOI: 10.17223/15617793/476/28.
24. Цзя Ш. Правовая защита права гражданина на изображение лица при применении технологии распознавания лиц в законодательстве Китая / Ш. Цзя, Ц. Чжан // *Правоведение*. – 2024. – Т. 68, № 2. – С. 271–283. – DOI: 10.21638/spbu25.2024.210.
25. Пономарева К. А. Правовые проблемы налогообложения цифровых бизнес-моделей / К. А. Пономарева // *Вестник Пермского университета. Юридические науки*. – 2022. – Вып. 58. – С. 605–620. – DOI: 10.17072/1995-4190-2022-58-605-620.

## REFERENCES

1. Kuteynikov D.L., Izhaev O.A., Lebedev V.A., Zenin S.S. Privacy in the realm of Artificial Intelligence Systems Application for Remote Biometric Identification. *Lex Russica*, 2022, vol. 75, no. 2, pp. 121–131. DOI: 10.17803/1729-5920.2022.183.2.121-131. (In Russ.).
2. Ablameyko M., Bogush R. Intelligent video surveillance in "smart city": control and protection of visual personal data. *Sudebnaya ekspertiza Belarusi = Forensic Examination of Belarus*, 2023, no. 1 (16), pp. 15–23. (In Russ.).
3. Mozhaeva S.Yu., Mozhaev S.A. About some issues of using biometric identification for the purposes of identifying crimes and offenses of supervised persons. *Vestnik Voronezhskogo instituta MVD Rossii = Vestnik of Voronezh institute of the Ministry of the interior of Russia*, 2024, no. 2, pp. 223–227. (In Russ.).
4. Bibri S.E., Krogstie J. A Novel Model for Data-Driven Smart Sustainable Cities of the Future: A Strategic Roadmap to Transformational Change in the Era of Big Data. *Future Cities and Environment*, 2021, vol. 7, art. 3. DOI: 10.5334/fce.116.
5. Benkő M., Bene B., Pirty Á., Szabó Á., Egedy T. Real vs. Virtual City: Planning Issues in a Discontinuous Urban Area in Budapest's Inner City. *Urban Planning*, 2021, vol. 6, no. 4, pp. 150–163. DOI: 10.17645/up.v6i4.4446.



6. Smith M., Miller S. The ethical application of biometric facial recognition technology. *AI & Society*, 2022, vol. 37, iss. 1, pp. 167–175. DOI: 10.1007/s00146-021-01199-9.
7. Mann M., Smith M. Automated facial recognition technology: Recent developments and approaches to oversight. *University of New South Wales Law Journal*, 2017, vol. 40, iss. 1, pp. 121–145. DOI: 10.53637/KAVV4291.
8. Kavoliūnaitė-Ragauskienė E. Right to Privacy and Data Protection Concerns Raised by the Development and Usage of Face Recognition Technologies in the European Union. *Journal of Human Rights Practice*, 2024, vol. 16, iss. 2, pp. 658–674. DOI: 10.1093/jhuman/huad065.
9. Babaeva Yu.G., Israelyan V.B. Biometrical image: legal regulation of a person's digital data. *Vestnik Universiteta Pravitel'stva Moskvyy = MMGU Herald*, 2022, no. 3 (57), pp. 17–23. (In Russ.).
10. Zatolokin A.A., Streltsov V.V. Administrative and legal aspects of state regulation of biometric personal data processing. *Obshchestvo i pravo = Society and Law*, 2023, no. 1 (83), pp. 79–83. (In Russ.).
11. Pereira R.S. Remarks on the Use of Biometric Data Systems (and Facial Recognition Technologies) for Law Enforcement Purposes: Security Implications of the Proposal for an EU Regulation on Artificial Intelligence, in: Moura Vicente D., de Vasconcelos Casimiro S., Chen C. (eds.). *The Legal Challenges of the Fourth Industrial Revolution. The European Union's Digital Strategy, Law, Governance and Technology Series*; vol. 57, Cham, Springer Publ., 2023, pp. 193–209. DOI: 10.1007/978-3-031-40516-7\_11.
12. Utegen D., Rakhmetov B.Zh. Facial Recognition Technology and Ensuring Security of Biometric Data: Comparative Analysis of Legal Regulation Models. *Journal of Digital Technologies and Law*, 2023, vol. 1, no. 3, pp. 825–844. DOI: 10.21202/jdtl.2023.36.
13. Kovaleva N., Zhirnova N. Issues of Ensuring the Confidentiality of Personal Data When Using Artificial Intelligence Systems. *Zhurnal Rossiiskogo prava = Journal of Russian Law*, 2024, vol. 28, no. 7, pp. 109–121. DOI: 10.61205/S160565900027561-1. (In Russ.).
14. Ryvkin S.Yu., Galkina V.A. Biometric technologies – a new level of human identification. *Moya professional'naya kar'era*, 2019, no. 7, vol. 4, pp. 90–95. (In Russ.).
15. Afanasev S.D., Tereshchenko I.A., Yatskevich D.A. Biometric identification and human rights: the line of demarcation. *Zakon*, 2022, no. 3, pp. 33–46. DOI: 10.37239/0869-4400-2022-18-3-33-46. (In Russ.).
16. Kolodenkova A.E. Ontology of human identification by face and body motions in video surveillance systems. *Ontologiya proektirovaniya = Ontology of Designing*, 2023, vol. 13, no. 1, pp. 55–74. DOI: 10.18287/2223-9537-2023-13-1-55-74. (In Russ.).
17. Mishchenko E.Y., Sokolov A.N. Model of Identification of a Person in Databases of Various Sizes, in: *2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBREIT)*, IEEE Publ., 2021, pp. 407–410. DOI: 10.1109/USBREIT51232.2021.9455020.
18. Ivanov V.A., Smirnov A.A., Nikolaev D.A. The real probability of recognizing images of people's faces using artificial neural networks. *Radiotekhnika*, 2022, vol. 86, no. 1, pp. 55–60. DOI: 10.18127/j00338486-202201-09. (In Russ.).
19. Krivogin M.S. Peculiarities of Legal Regulating Biometric Personal Data. *Pravo. Zhurnal Vysshei shkoly ekonomiki = Law. Journal of the Higher School of Economics*, 2017, no. 2, pp. 80–89. (In Russ.).
20. Jaiswal A., Tarar S. Real-Time Biometric System for Security and Surveillance Using Face Recognition, in: Singh M., Gupta P., Tyagi V., Flusser J., Ören T., Valentino G. (eds.). *Advances in Computing and Data Sciences*, 4th International Conference, ICACDS 2020, Valletta, Malta, April 24–25, 2020, Revised Selected Papers, Communications in Computer and Information Science; vol. 1244, Singapore, Springer Publ., 2020, pp. 293–304. DOI: 10.1007/978-981-15-6634-9\_27.
21. Fabrègue B.F.G., Bogoni A. Privacy and Security Concerns in the Smart City. *Smart Cities*, 2023, vol. 6, iss. 1, pp. 586–613. DOI: 10.3390/smartcities6010027.
22. Gupta S., Modgil S., Lee C.K., Sivarajah U. The future is yesterday: Use of AI-driven facial recognition to enhance value in the travel and tourism industry. *Information Systems Frontiers*, 2023, vol. 25, iss. 3, pp. 1179–1195. DOI: 10.1007/s10796-022-10271-8.
23. Kuznetsova S.S., Mochalov A.N., Salikov M.S. Biometric identification on the Internet: Trends of legal regulation in Russia and in foreign countries. *Vestnik Tomskogo gosudarstvennogo universiteta = Tomsk State University Journal*, 2022, no. 476, pp. 257–267. DOI: 10.17223/15617793/476/28. (In Russ.).

24. Jia S., Zhang J. Legal protection of a citizen's right to a facial image when applying facial recognition technology in Chinese law. *Pravovedenie*, 2024, vol. 68, no. 2, pp. 271–283. DOI: 10.21638/spbu25.2024.210. (In Russ.).

25. Ponomareva K.A. Legal Issues of Taxation of Digital Business Models. *Vestnik Permskogo universiteta. Yuridicheskie nauki = Perm University Herald. Juridical Sciences*, 2022, iss. 58, pp. 605–620. DOI: 10.17072/1995-4190-2022-58-605-620. (In Russ.).

#### ИНФОРМАЦИЯ ОБ АВТОРАХ

**Чурикова Анна Юрьевна** – кандидат юридических наук, доцент, <sup>1</sup>доцент кафедры информационного права и цифровых технологий, <sup>2</sup>ведущий научный сотрудник

<sup>1</sup> *Саратовская государственная юридическая академия*

<sup>2</sup> *Государственный университет управления*

<sup>1</sup> 410056, Россия, г. Саратов, ул. Вольская, 1

<sup>2</sup> 109542, Россия, г. Москва, Рязанский пр., 99

E-mail: a\_tschurikova@bk.ru

ORCID: 0000-0003-0299-622X

ResearcherID: AAV-8381-2020

Scopus AuthorID: 58251251000

SPIN-код РИНЦ: 9809-3156; AuthorID: 713265

**Липчанская Мария Александровна** – доктор юридических наук, профессор, <sup>1</sup>профессор кафедры конституционного права имени Н.В. Витрука, <sup>2</sup>профессор кафедры государственно-правовых дисциплин ИГСУ

<sup>1</sup> *Российский государственный университет правосудия*

<sup>2</sup> *Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации*

<sup>1</sup> 117418, Россия, г. Москва, ул. Новочеремушкинская, 69

<sup>2</sup> 119602, Россия, г. Москва, пр. Вернадского, 82

E-mail: lipchan\_maria@mail.ru

ORCID: 0000-0002-4410-0578

ResearcherID: ABC-6179-2020

Scopus AuthorID: 57218912583

SPIN-код РИНЦ: 9665-2557; AuthorID: 360796

#### БИБЛИОГРАФИЧЕСКОЕ ОПИСАНИЕ СТАТЬИ

Чурикова А.Ю. Проблемы использования биометрических технологий в муниципальных образованиях / А.Ю. Чурикова, М.А. Липчанская // *Правоприменение*. – 2025. – Т. 9, № 3. – С. 64–73. – DOI: 10.52468/2542-1514.2025.9(3).64-73.

#### INFORMATION ABOUT AUTHORS

**Anna Yu. Churikova** – PhD in Law, Associate Professor; <sup>1</sup>Associate Professor, Department of Information Law and Digital Technologies; <sup>2</sup>leading researcher

<sup>1</sup> *Saratov State Law Academy*

<sup>2</sup> *State University of Management*

<sup>1</sup> 1, Vol'skaya ul., Saratov, 410056, Russia

<sup>2</sup> 99, Ryazanskii pr., Moscow, 109542, Russia

E-mail: a\_tschurikova@bk.ru

ORCID: 0000-0003-0299-622X

ResearcherID: AAV-8381-2020

Scopus AuthorID: 58251251000

RSCI SPIN-code: 9809-3156; AuthorID: 713265

**Maria A. Lipchanskaya** – Doctor of Law, Professor; <sup>1</sup>Professor, Department of Constitutional Law named after N.V. Vitruk; <sup>2</sup>Professor, Department of State and Legal Disciplines of the Institute of Social and Cultural Studies

<sup>1</sup> *Russian State University of Justice*

<sup>2</sup> *Russian Presidential Academy of National Economy and Public Administration*

<sup>1</sup> 69, Novocheremushkinskaya ul., Moscow, 117418, Russia

<sup>2</sup> 82, Vernadskogo pr., Moscow, 119602, Russia

E-mail: lipchan\_maria@mail.ru

ORCID: 0000-0002-4410-0578

ResearcherID: ABC-6179-2020

Scopus AuthorID: 57218912583

RSCI SPIN-code: 9665-2557; AuthorID: 360796

#### BIBLIOGRAPHIC DESCRIPTION

Churikova A.Yu, Lipchanskaya M.A. Problems of using biometric technologies in municipalities. *Pravoprime-nenie = Law Enforcement Review*, 2025, vol. 9, no. 3, pp. 64–73. DOI: 10.52468/2542-1514.2025.9(3).64-73. (In Russ.).