

Научная статья

Научная специальность

5.1.2 «Публично-правовые (государственно-правовые) науки»

УДК 342.951:351.82

DOI <https://doi.org/10.26516/2071-8136.2025.3.34>

ОГРАНИЧЕНИЯ ПУБЛИЧНО-ПРАВОВОЙ ЗАЩИТЫ БИОМЕТРИИ В РАМКАХ ЕДИНОЙ БИОМЕТРИЧЕСКОЙ СИСТЕМЫ

© Митянов З. О., 2025

Нижегородский филиал Национального исследовательского университета «Высшая школа экономики»,
г. Нижний Новгород, Россия

Рассматривается сложившийся механизм публично-правовой защиты биометрических персональных данных в рамках Единой биометрической системы (ЕБС). Анализируются его основные проблемы в контексте запрета обработки биометрии вне ЕБС. Акцентируется внимание на проблемах ограниченности круга биометрических идентификаторов, обрабатываемых в ЕБС, и ограниченности техник обработки биометрии идентификацией и аутентификацией, приводятся иные сопутствующие проблемы. Делаются выводы о необходимости унификации всех разновидностей и техник обработки биометрии в рамках ЕБС; ужесточения правил обращения с биометрией в случае допущения ее обработки вне ЕБС в течение переходного периода; дополнения законодательства дефинициями и нормами о регулировании биометрических техник распознавания и категоризации; выработки единого риск-ориентированного подхода к публично-правовой защите биометрии в России.

Ключевые слова: биометрические персональные данные, публично-правовая защита, Единая биометрическая система, биометрические идентификаторы, биометрические техники.

LIMITATIONS OF PUBLIC-LAW PROTECTION OF BIOMETRICS WITHIN THE FRAMEWORK OF THE UNIFIED BIOMETRIC SYSTEM

© Mitianov Z. O., 2025

Nizhny Novgorod Branch of the National Research University Higher School of Economics,
Nizhny Novgorod, Russian Federation

The article examines the existing mechanism of public-law protection of biometric personal data within the framework of the Unified Biometric System (UBS). Its main problems are analyzed in the context of the prohibition on processing biometrics outside the UBS. Attention is focused on the problems of the limited range of biometric identifiers processed in the UBS, and the limited techniques for processing biometrics, also other related problems are given. Conclusions are made about the need to unify all types of biometric identifiers and techniques of processing within the UBS; to tightening the rules for handling biometrics in the event that their processing is permitted outside the UBS during the transition period; to supplementing the legislation with definitions and norms on the regulation of biometric recognition and categorization techniques; to developing a unified risk-oriented approach to the public-law protection of biometrics in Russia.

Keywords: biometric personal data, public-law protection, Unified Biometric System, biometric identifiers, biometric techniques.

Введение

Масштабы сбора и обработки биометрических персональных данных (далее – БПД) растут с каждым годом¹. Этому способствует популярность биометрических систем: онлайн-банкинг, управление доступом (например, проход в фитнес-клуб), оплата товаров и услуг и многие иные операции упрощаются благодаря развитию биометрии. Однако нельзя забы-

вать, что БПД уязвимы по своей природе. Их уязвимость объясняется тем, что, согласно действующему определению, они характеризуют сведения о физиологических и биологических особенностях человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных. Данные особенности человека чаще всего неизменны на протяжении всей его жизни. Именно поэтому утечка, подделка и компрометация БПД ставят под угрозу безопасность «цифрового облика», выливаясь не только в деанонимизацию, но и

¹ Биометрические технологии расширяют ареал обитания // Ведомости. URL: <https://www.vedomosti.ru/technologies/trendsrub/articles/2025/05/27/1112220-rasshiryayut-areal-obitaniya> (дата обращения: 15.06.2025).

поддельную идентификацию (или аутентификацию) человека и связанные с ними юридические и моральные негативные последствия [4, с. 110]. БПД требуют особой правовой защиты со стороны органов публичной власти, более строгой в сравнении с иными категориями персональных данных.

По состоянию на конец 2024 г., согласно данным ВЦИОМ¹, 68 % россиян знакомы с понятием «биометрия». При этом четверо из десяти опрошенных относятся к биометрической идентификации положительно, 29 % отрицательно, 25 % нейтрально. В вопросах хранения и обработки БПД 42 % доверяют только государственным учреждениям, только коммерческим всего 2 %; не доверяют никому 44 %. Наблюдается устойчивый рост заинтересованности и доверия населения к рынку биометрии (по сравнению с 2023 г.), в особенности к государственным системам, таким как Единая биометрическая система (далее – ЕБС). Тем не менее немалый процент населения (54 %) видит утечку БПД опасной и способной нанести существенный вред.

Превалирующим и наиболее эффективным видом правовой защиты БПД является их публично-правовая защита (далее – ППЗ), которая представляет собой деятельность органов публичной власти, реализуемую путем правотворчества и правоприменения, направленную на обеспечение реальной возможности осуществления субъективных прав, восстановление нарушенных и (или) оспариваемых прав и законных интересов. ППЗ наиболее эффективна для защиты БПД, поскольку негосударственные виды правовой защиты не обеспечивают должного уровня безопасности таких уязвимых данных, особенно с учетом отсутствия инструментов властного принуждения.

При этом ППЗ осуществляется через инструменты, т. е. совокупность правовых средств, процедур и институтов, обеспечивающих достижение ее цели. А. В. Малько отмечает, что инструменты являются рабочим механизмом системы, связывая установленные нормативные правила с практикой их реализации [2]. Инструменты ППЗ БПД делятся на несколько видов в зависимости от их функционального назначения. Так, можно выделить нормативные правовые (законы и подзаконные акты), институциональные (уполномоченные органы государственной власти, например Роскомнад-

зор), процессуальные, санкционные (например, административная ответственность за правонарушения в сфере обработки БПД) и технико-правовые (например, технические стандарты защиты БПД) инструменты ППЗ БПД. В работе будут рассматриваться преимущественно проблемы нормативно-правовых и институциональных инструментов ППЗ БПД.

Механизм ППЗ БПД реализуется как в деятельности правоохранительных органов, так и при оказании государственных/муниципальных услуг, в банковской сфере и иных сферах повседневной жизни граждан. Отличие в том, что в первом случае обработка БПД осуществляется практически всегда без согласия субъекта в целях реализации публичного интереса и происходит она в специализированных информационных системах; такой порядок обработки БПД можно назвать «принудительной» биометрией [3, с. 67], он нормативно обособлен и имеет свои особенности реализации. Во втором же случае обработка БПД осуществляется добровольно с согласия субъекта БПД и происходит она с 2022 г. исключительно² в рамках формирования и функционирования Единой биометрической системы (далее – ЕБС); данный порядок условно характеризуется как «добровольная» биометрия [Там же, с. 68].

В нашей работе будет рассматриваться механизм ППЗ БПД в рамках ЕБС, поскольку он появился относительно недавно, более динамичен, прозрачен (в сравнении с «принудительной» биометрией) и перспективен для изучения. Кроме того, сама «добровольная» биометрия ближе к повседневной жизни рядового гражданина, и от эффективности ее регулирования зависит общий уровень доверия граждан к биометрии, а также устойчивость развития данного рынка в России.

Ограниченность перечня биометрических идентификаторов, размещаемых и обрабатываемых в ЕБС

Легальное определение БПД, содержащееся в ст. 11 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»³ (далее – ФЗ № 152-ФЗ), относит к ним сведения о физиологических и биологических особенностях человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта пер-

¹ Биометрия на марше: лицом к лицу с будущим // ВЦИОМ. Новости. URL: <https://wciom.ru/analytical-reviews/analiticheskii-obzor/biometrija-na-marshe-licom-k-licu-s-budushchim> (дата обращения: 17.06.2025).

² Под исключительностью в данном случае подразумевается фактический запрет обработки БПД вне ЕБС, установленный ст. 15 ФЗ № 152-ФЗ.

³ О персональных данных : федер. закон от 27.07.2006 № 152-ФЗ // Собр. законодательства РФ. 2006. № 31 (ч. 1). Ст. 3451.

сональных данных. Физиологических и биологических особенностей человека, достаточных для его идентификации и/или аутентификации, достаточно много. Их перечень не закреплен в действующем законодательстве РФ, однако существуют разъяснения компетентных органов, а также доктринальные позиции и зарубежный опыт по отнесению тех или иных сведений к БПД.

Во-первых, согласно письму Минцифры России от 17 июля 2020 г. № ОП-П24-070-19433¹ и письму Роскомнадзора от 10 февраля 2020 г. № 08АП-6782², к БПД могут относиться фотографическое изображение человека (используемое для установления личности, например, фото на пропуске), видеоизображение человека, дактилоскопические данные, информация о радужной оболочке глаза, результаты анализов ДНК и данные о голосе. Указанный перечень не является исчерпывающим, а служит, скорее, ориентиром для понимания примерного состава БПД. Доктрина и зарубежные правовые порядки [7] также относят к БПД данные о группе крови, почерк, манеру набора на клавиатуре, манеру походки, особенности мимики и жестикуляции, рисунок вен ладони и множество иных данных³, включая даже характеристики ауры человека [1].

Во-вторых, согласно ч. 4 ст. 3 Федерального закона 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»⁴ (далее – ФЗ № 572-ФЗ) в ЕБС размещаются и обрабатываются изображение лица человека и запись голоса человека, при этом полный перечень видов БПД, размещаемых и обрабатываемых в ЕБС, закреплен в

постановлении Правительства РФ от 1 апреля 2024 г. № 408 «О видах биометрических персональных данных, на которые распространяется действие Федерального закона “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”»⁵. Перечень, установленный в нем, на настоящий момент дублирует положения ч. 4 ст. 3 ФЗ № 572-ФЗ и актуален с 1 сентября 2024 г. до 1 сентября 2027 г. Об обработке иных видов БПД в рамках ЕБС речи не идет. При этом ст. 15 ФЗ № 572-ФЗ запрещает обработку и хранение БПД в коммерческих информационных системах (т. е. вне ЕБС).

В итоге создается уникальная противоречивая ситуация. С одной стороны, обработка и хранение БПД в коммерческих информационных системах (далее – КИС) в целях идентификации и/или аутентификации вне ЕБС запрещены. С другой стороны, в ЕБС на данный момент могут обрабатываться лишь изображение лица и запись голоса. Обработка многих иных видов БПД «подвисает в воздухе», поскольку формально она запрещена вне ЕБС, но и в ЕБС осуществляться не может.

Сложившейся неопределенностью пользуются недобросовестные операторы БПД, считающие, что отсутствие закрепления иных видов биометрических идентификаторов (помимо лица и голоса) в порядке обработки в рамках ЕБС предоставляет «лазейку» для обработки в общем порядке (по ст. 11 ФЗ № 152-ФЗ, т. е. с письменного согласия лица, в собственной базе данных). Например, деятельность операторов домофонов, предусматривающих доступ по отпечатку пальца (взамен изображения лица или записи голоса), не подпадает под действие ФЗ № 572-ФЗ и может осуществляться в общем порядке обработки БПД без подключения к ЕБС. На это указывается в Письме Минцифры от 28 декабря 2023 г. № П24-2-04-070-257558⁶.

⁵ О видах биометрических персональных данных, на которые распространяется действие Федерального закона «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»: постановление Правительства РФ от 1 апр. 2024 г. № 408 // Собр. законодательства РФ. 2024. № 15. Ст. 2042.

⁶ О направлении информации: письмо Минцифры России от 28.12.2023 № П24-2-04-070-257558 // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_468549/ (дата обращения: 29.06.2025).

¹ О рассмотрении обращения: письмо Минцифры России от 17 июля 2020 г. № ОП-П24-070-19433 // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_393140/ (дата обращения: 28.06.2025).

² О направлении информации по протоколу совещания: письмо Роскомнадзора от 10 февр. 2020 г. № 08АП-6782 (вместе с «Практическими рекомендациями по применению положений Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» при обработке биометрических персональных данных несовершеннолетних») // КонсультантПлюс. URL: https://www.consultant.ru/document/cons_doc_LAW_393146/ (дата обращения: 28.06.2025).

³ Типы биометрии: полное руководство // РЕКФЭИСИС. URL: <https://recfaces.ru/articles/types-of-biometrics> (дата обращения: 25.06.2025).

⁴ 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: федер. закон от 29 дек. 2022 г. № 572-ФЗ // Собрание законодательства РФ. 2023. № 1 (ч. 1). Ст. 19.

Подобные «лазейки» создают большие угрозы для иных видов БПД, помимо изображения лица и записи голоса, поскольку в законодательстве отсутствует градация уязвимости БПД.

На сегодняшний день путей решения сложившейся неопределенности как минимум два. Обработка иных видов БПД может быть объявлена «вне закона», что противоречит ориентиру на содействие прогрессу технологий и ставит под угрозу развитие целой отрасли биометрии, но при этом устраняет риски обходных путей обработки таких БПД. В ином случае обработка иных видов БПД может осуществляться в общем порядке согласно правилам ФЗ № 152-ФЗ и окончательно отделиться от правил обработки в рамках ЕБС. Во втором сценарии наиболее волнующим вопросом становится обеспечение единообразия правил и безопасности обработки и хранения таких БПД, ведь при допущении легальной обработки БПД вне ЕБС стандарты их получения, хранения, передачи и уничтожения должны быть не ниже аналогичных требований по обработке БПД в рамках ЕБС.

Оба сценария видятся допустимыми и обусловлены скорее уровнем развития и массовостью применения биометрических технологий, однако во избежание путаницы и «разброса» БПД по различным информационным системам целесообразнее все же унифицировать порядок обработки всех возможных разновидностей БПД в рамках ЕБС.

Ограниченность техник обработки биометрических персональных данных

Важно понимать, что помимо идентификации и аутентификации современные технологии (в том числе искусственный интеллект) позволяют производить с БПД иные операции, например категоризацию и распознавание, которые не урегулированы российским правом.

Технологии или операции, основанные на специальной технической обработке БПД, в современной зарубежной практике именуются биометрическими техниками [10]. Согласно классификации, созданной при разработке Регламента Европейского союза об искусственном интеллекте¹ (далее – AI Act), для обработки БПД могут применяться четыре биометрические техники: распознавание (biometric recognition),

категоризация (biometric categorization), идентификация (biometric identification) и аутентификация (biometric verification). В качестве ориентира рассматривается опыт ЕС, поскольку именно там было впервые предложено систематизированное правовое регулирование новейших техник.

Текущий понятийный аппарат российского законодательства сосредоточен лишь на аутентификации и идентификации по БПД и не учитывает всего многообразия биометрических техник. Российский законодатель по смыслу легального определения (ст. 11 ФЗ № 152-ФЗ) указывает только на возможность аутентификации или идентификации лица по БПД, поскольку данные техники используются непосредственно для установления личности. Кроме того, ФЗ № 572-ФЗ в своем названии и содержании оперирует только указанными понятиями. Для распознавания и категоризации в России отсутствует правовое регулирование. Нормы ФЗ № 152-ФЗ и ФЗ № 572-ФЗ не содержат положений о группировке людей по биометрическим параметрам, равно как о допустимости распознавания эмоций и намерений. В этой связи общее правило об обработке БПД с письменного согласия видится устаревшим, поскольку распознавание и категоризация могут применяться скрыто [6, р. 785]; согласие также можно обойти, поскольку в легальном определении БПД не идет о речи об иных биометрических техниках, кроме идентификации и аутентификации, что позволяет применять распознавание и категоризацию без ограничений.

Для поиска возможных вариантов ППЗ БПД при применении техник распознавания и категоризации в рамках ЕБС стоит обратить внимание на европейский опыт. В недавно принятом AI Act ЕС содержатся определения и характеристики всех четырех техник. Особый интерес для изучения представляют именно определения распознавания и категоризации, так как дефиниции идентификации и аутентификации схожи с российскими по смыслу и порядку изложения.

Согласно ст. 3(39) AI Act, биометрическое распознавание – это определение или предсказывание эмоций или намерений физических лиц системой ИИ на основе их биометрических данных. При этом преамбула 18 содержит перечень таких эмоций и намерений, среди которых гнев, волнение, удивление, движение головы, шепот, нахмуренный взгляд и другие. То есть системы ИИ уже способны не просто идентифицировать

¹ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13.06.2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) № 300/2008, (EU) № 167/2013, (EU) № 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) // EUR-Lex. URL: <http://data.europa.eu/eli/reg/2024/1689/oj> (дата обращения: 27.06.2025).

и аутентифицировать человека, но и распознать его эмоции и намерения. Риски от применения распознавания велики: нарушение права на неприкосновенность частной жизни, ложные подозрения, дискриминация, манипулирование потребительским поведением и искажение поведения людей (т. е. люди, предварительно зная либо догадываясь о применении в отношении них биометрического распознавания, могут намеренно либо инстинктивно изменять свое поведение на более нейтральное, находясь «под прицелом камер») [10]. Для защиты граждан AI Act в ст. 5(1)(f) запрещает применение распознавания в местах работы и учебы за исключением использования по соображениям медицины и безопасности.

В ст. 3(40) AI Act также содержится определение биометрической категоризации, подразумевающее под данной техникой отнесение системой ИИ физических лиц к определенным категориям на основе их биометрических данных, если оно не является вспомогательной услугой и технической необходимостью. Преамбула 16 относит к таким категориям пол, возраст, цвет волос, татуировки, поведенческие или личностные особенности, религию и иные характеристики. Риски от группировки людей на основе БПД не менее существенны: дискриминация, стигматизация («клеймение») [9], нарушение права на самоопределение и неприкосновенность частной жизни [8]. Применение категоризации запрещено нормой ст. 5(1)(g) AI Act, за исключением маркировки/сортировки законно полученных БПД либо ее применения правоохранительными органами.

На начальном этапе, для имплементации рассмотренных выше институтов в российское законодательство, стоит дополнить легальную дефиницию БПД, расширив перечень возможных операций с ними. Например, можно указать, что БПД – это сведения, которые характеризуют физиологические, биологические и поведенческие особенности человека, на основании которых можно установить его личность, отнести его к определенной группе (категории) либо определить (предсказать) его эмоции и намерения, и которые могут служить либо используются оператором для аутентификации, идентификации, категоризации или распознавания. Кроме того, необходимо детально изучить пути взаимной интеграции новейших техник обработки БПД и ЕБС.

Вторым этапом совершенствования ППЗ БПД мог бы стать запрет применения наиболее

высокорисковых техник. В частности, целесообразно введение законодательного запрета применения распознавания, категоризации и идентификации на основе ИИ, в особенности хозяйствующими субъектами (например, крупными корпорациями), во избежание массовой слежки и манипулирования потребительским поведением. Не менее важно ввести ограничения на биометрическую аутентификацию на основе ИИ. Необходимо уточнить, что введение подобных запретов целесообразно лишь в области «добровольной» биометрии для защиты повседневной жизни граждан от чрезмерного вмешательства со стороны. Безусловно, предлагаемые запреты не должны распространяться на применение новейших техник на основе ИИ в области «принудительной» биометрии: в правоприменительной сфере (в том числе в деятельности правоохранительных органов), сфере безопасности (государственной, транспортной, объектов критической инфраструктуры, режимных объектов) и сфере здравоохранения.

Заключение

В завершение рассмотрения основных проблем и ограничений ППЗ БПД в рамках ЕБС будут приведены выводы о пробелах и возможных путях реформирования российского законодательства.

На настоящий момент существует два основных ограничения обработки БПД в рамках ЕБС: узкий перечень биометрических идентификаторов (только изображение лица и запись голоса человека) и ограниченность техник (операций) обработки БПД. Вероятными путями устранения данных пробелов могут стать следующие действия.

Во-первых, необходима скорейшая унификация подхода к ППЗ всех видов БПД, которая может быть достигнута путем расширения перечня БПД, размещаемых и обрабатываемых в ЕБС (со включением туда наиболее распространенных видов БПД помимо лица и голоса). Во-вторых, на текущем переходном этапе возможно рассмотрение вопроса о допустимости обработки БПД вне ЕБС (т. е. в КИС) в строго определенных целях и с соблюдением установленных стандартов безопасности, сопоставимых с ЕБС; тем не менее видится, что основную ставку в будущем стоит сделать на унификацию обработки всей биометрии в рамках ЕБС. В-третьих, целесообразно детализировать законодательство о БПД, дополнив его нормами о правовом регулировании новейших техник обработки БПД, таких как ка-

тегоризация и распознавание; в частности, установить легальные дефиниции биометрических распознавания и категоризации, проработать пути интеграции данных техник в ЕБС, а также установить выборочные запреты на применение распознавания, категоризации, идентификации и аутентификации по биометрии с использованием ИИ в области «добровольной» биометрии. В конечном счете подход к ППЗ БПД в России стоит реформировать в русле риск-ориентированности и точечного регулирования проблем, возникающих ввиду стремительного развития технологий (схожий подход в настоящее время реализуется в Китае) [5].

В конце стоит сказать, что унификация и детализация подхода ППЗ БПД в России может не только обеспечить их безопасность, но и способствовать устойчивому развитию перспективного рынка биометрии, призванного в первую очередь упростить повседневную жизнь граждан и бизнеса в рамках развития цифровой экономики. 

СПИСОК ЛИТЕРАТУРЫ

1. Иванский В. П. Информация об ауре человека как объект правового регулирования Федерального закона «О персональных данных» // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2015. № 3. С. 34–45.
2. Малько А. В., Саломатин А. Ю. Теория государства и права : учеб. пособие. 3-е изд. М. : ИНФРА-М, 2024. 213 с.
3. Митянов З. О. Принудительная и добровольная биометрия: содержание и разграничение в российском праве // Теоретическая и прикладная юриспруденция. 2024. № 3. С. 63–74. DOI: 10.22394/3034-2813-2024-3-63-74
4. Рассолов И. М., Чубукова С. Г., Микурова И. В. Биометрия в контексте персональных данных и генетической информации: правовые проблемы // Lex Russica (Русский закон). 2019. № 1 (146). С. 108–118. DOI: 10.17803/1729-5920.2019.146.1.108-118
5. Филипова И. А. Правовое регулирование искусственного интеллекта: опыт Китая // Journal of Digital Technologies and Law. 2024. Т. 2, № 1. С. 46–73. DOI: 10.21202/jdtl.2024.4
6. Durovic M., Watson J. Nothing to Be Happy about: Consumer Emotions and AI // Scispace. 2021. N 4 (4). P. 784–793. DOI: 10.3390/j4040053
7. Jain A. K., Ross A., Nandakumar K. Introduction to Biometrics. New York : Springer, 2016. 312 p. DOI: 10.1007/978-0-387-77326-1
8. Kuteynikov D. L., Izhaev O. A. Analysing Risk-Based Approach in the Draft EU Artificial Intelligence Act // Legal Issues in the Digital Age. 2023. N 3. P. 97–116. DOI: 10.17323/2713-2749.2023.3.97.116
9. Subotić I. Implications of EU's artificial intelligence Act // Znanstvena Misel. 2024. N 86. P. 7–13.
10. Wendehorst C. Biometric Recognition and Behavioural Detection: Assessing the Ethical Aspects of Biometric Recognition and Behavioural Detection Techniques with a Focus on Their Current and Future Use in Public Spaces (Study) / ed. by C. Wendehorst, Y. Duller // Think Tank. URL: <https://www.europarl.europa.eu>.

REFERENCES

1. Ivanskii V.P. Informatsiya ob aure cheloveka kak ob'ekt pravovogo regulirovaniya Federalnogo zakona "O personalnykh dannykh" [Information on human aura as an object of legal regulation of the federal law "On personal data"]. *Vestnik Rossiiskogo universiteta druzhby narodov. Seriya: Yuridicheskie nauki* [RUDN journal of law], 2015, no. 3, pp. 34–45. (in Russian)
2. Malko A.V., Salomatin A.Yu. *Teoriya gosudarstva i prava* [Theory of state and law]. Textbook. 3rd ed. Moscow, INFRA-M Publ., 2024. 213 p. (in Russian)
3. Mitianov Z.O. Prinuditelnaya i dobrovolnaya biometriya: soderzhanie i razgranichenie v rossiiskom prave [Compulsory and voluntary biometrics: content and distinction in Russian law]. *Teoreticheskaya i prikladnaya yurisprudentsiya* [Theoretical and applied law], 2024, no. 3, pp. 63–74. DOI: 10.22394/3034-2813-2024-3-63-74 (in Russian)
4. Rassolov I.M., Chubukova S.G., Mikurova I.V. Biometriya v kontekste personal'nykh dannykh i geneticheskoi informatsii: pravovye problemy [Biometrics in the context of personal data and genetic information: legal issues]. *Lex Russica* [The Russian law], 2019, no. 1 (146), pp. 108–118. DOI: 10.17803/1729-5920.2019.146.1.108-118 (in Russian)
5. Filipova I.A. Pravovoe regulirovanie iskusstvennogo intellekta: opyt Kitaya [Legal regulation of artificial intelligence: experience of China]. *Journal of Digital Technologies and Law*, 2024, vol. 2, no. 1, pp. 46–73. DOI: 10.21202/jdtl.2024.4 (in Russian)
6. Durovic M., Watson J. Nothing to Be Happy about: Consumer Emotions and AI. *Scispace*, 2021, vol. 4, no. 4, pp. 784–793. DOI: 10.3390/j4040053
7. Jain A.K., Ross A., Nandakumar K. *Introduction to Biometrics*. New York, Springer, 2016, 312 p. DOI: 10.1007/978-0-387-77326-1
8. Kuteynikov D.L., Izhaev O.A. Analysing Risk-Based Approach in the Draft EU Artificial Intelligence Act. *Legal Issues in the Digital Age*, 2023, no. 3, pp. 97–116. DOI: 10.17323/2713-2749.2023.3.97.116
9. Subotić I. Implications of EU's artificial intelligence Act. *Znanstvena Misel*, 2024, no. 86, pp. 7–13.
10. Wendehorst C. Biometric Recognition and Behavioural Detection: Assessing the Ethical Aspects of Biometric Recognition and Behavioural Detection Techniques with a Focus on Their Current and Future Use in Public Spaces (Study). Group of authors; ed. by C. Wendehorst, Y. Duller. *Think Tank*. Available at: <https://www.europarl.europa.eu>.

Статья поступила в редакцию 09.07.2025; одобрена после рецензирования 21.08.2025; принята к публикации 03.09.2025

Received on 09.07.2025; approved on 21.08.2025; accepted for publication on 03.09.2025

Митянов Захар Олегович – аспирант, факультет права, Нижегородский филиал Национального исследовательского университета «Высшая школа экономики» (Россия, 603014, г. Нижний Новгород, Сормовское шоссе, 30), РИНЦ Author ID: 8851-7040, ORCID: 0009-0004-6764-7471, e-mail: zmityanov@hse.ru

Mitianov Zakhar Olegovich – Postgraduate, Faculty of Law, Nizhny Novgorod Branch of the National Research University Higher School of Economics (30, Sormovskoye highway, Nizhny Novgorod, 603014, Russian Federation), RSCI Author ID: 8851-7040, ORCID: 0009-0004-6764-7471, e-mail: zmityanov@hse.ru