

Обработка биометрических персональных данных в информационных системах работодателя: принципы и ограничения

Аннотация. В статье проводится сравнительно-правовой анализ регулирования обработки биометрических данных работников в Российской Федерации и странах Европейского Союза. Выявляется ключевая проблема: российская правовая модель, формально провозглашающая приоритет согласия субъекта, на практике допускает широкие исключения, оправдываемые государственными и корпоративными интересами, без надлежащей проверки их соразмерности. Это приводит к эрозии сферы частной автономии личности и создает риски установления гиперконтроля над сотрудниками. Европейская модель, основанная на Общем регламенте по защите данных Европейского Союза, создает более сбалансированный режим, где запрет является правилом, а любое исключение должно быть строго обосновано и подкреплено такими принципами, как пропорциональность, минимизация данных, прозрачность и безопасность. Ключевым инструментом соблюдения этих принципов является обязательная оценка воздействия на защиту данных (Data Protection Impact Assessment). Автор обосновывает необходимость совершенствования российского законодательства рисками нарушения конституционного принципа уважения человека труда, права на неприкосновенность частной жизни и фундаментальной задачей государства по обеспечению свободы личности. В заключение предлагаются конкретные меры по совершенствованию российского законодательства, в частности внедрение обязательной оценки воздействия обработки данных и разработка специализированных методических рекомендаций для работодателей.

Ключевые слова: биометрические персональные данные; персональные данные; Общий регламент по защите данных (General Data Protection Regulation, GDPR); оценка воздействия; принцип пропорциональности; принцип минимизации данных; трудовые отношения; цифровые права работника; увольнение; мониторинг исполнения трудовых обязанностей

Для цитирования: Менкенов А. В. Обработка биометрических персональных данных в информационных системах работодателя: принципы и ограничения // Актуальные проблемы российского права. — 2026. — Т. 21. — № 9. — С. 110–118. — DOI: 10.17803/1994-1471.2026.190.9.110-118

© Менкенов А. В., 2026

* Менкенов Алексей Владимирович, кандидат юридических наук, доцент кафедры междисциплинарных исследований и программ отделения «Высшая школа правоведения» Института права и национальной безопасности Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации
просп. Вернадского, д. 84, корп. 3, г. Москва, Российская Федерация, 119571
menkenov@ranepa.ru

Biometric Personal Data Processing in Employer Information Systems: Principles and Limitations

Alexey V. Menkenov, Cand. Sci. (Law), Associate Professor, Department of Interdisciplinary Research and Programs, Higher School of Law, Institute of Law and National Security, The Russian Presidential Academy of National Economy and Public Administration (RANEPA), Moscow, Russian Federation
menkenov@ranepa.ru

Abstract. The paper provides a comparative legal analysis of the regulation of the processing of biometric data of employees in the Russian Federation and the countries of the European Union. A key problem emerges: the Russian legal model, while formally declaring the priority of the subject's consent, in practice allows for broad exceptions justified by state and corporate interests, without proper verification of their proportionality. This leads to the erosion of the individual's sphere of private autonomy and creates the risk of establishing hyper-control over employees. The European model, based on the General Data Protection Regulation (GDPR), establishes a more balanced regime where prohibition is the rule, and any exception must be strictly justified and supported by principles such as proportionality, data minimization, transparency, and security. A key tool for complying with these principles is the mandatory data protection impact assessment (DPIA). The author substantiates the need to improve Russian legislation, arguing that this entails the risks of violating the constitutional principle of respect for working people, the right to privacy, and the fundamental duty of the state to ensure personal freedom. In conclusion, specific measures are proposed to improve Russian legislation, in particular the introduction of mandatory data processing impact assessments and the development of specialized methodological recommendations for employers.

Keywords: biometric personal data; personal data; GDPR; General Data Protection Regulation; impact assessment; proportionality principle; data minimization principle; labor relations; digital employee rights; dismissal; performance monitoring

Cite as: Menkenov AV. Biometric Personal Data Processing in Employer Information Systems: Principles and Limitations. *Aktual'nye problemy rossijskogo prava*. 2026;21(9):110-118. (In Russ.). DOI: 10.17803/1994-1471.2026.190.9.110-118

Введение

Стремительное развитие биометрических систем и технологий обработки данных трансформирует современные системы аутентификации и идентификации. Биометрическая безопасность становится неотъемлемым элементом корпоративных процессов, предлагая эффективный способ подтверждения личности работника. Обработка биометрических персональных данных основана на сборе и анализе физических, физиологических или поведенческих характеристик физических лиц с помощью технических средств с последующим созданием

биометрических шаблонов. Эти шаблоны позволяют работодателям идентифицировать, отслеживать и профилировать сотрудников зачастую без прямого и осознанного взаимодействия с человеком.

Биометрические персональные данные представляют собой неотчуждаемый и неотменяемый элемент идентичности человека, неконтролируемое распространение которого может иметь необратимые последствия¹. В отличие от сменяемых идентификаторов (паролей, кодов), биометрические характеристики индивидуальны и трудноизменяемы. Следовательно, в случае их утери или несанкциониро-

¹ Person identification, human rights and ethical principles: Rethinking biometrics in the era of artificial intelligence (PE 697.191, December 2021) / European Parliamentary Research Service ; Scientific Foresight Unit. European Union, 2021. P. 32.

ванного доступа они считаются безвозвратно скомпрометированными, что ставит под угрозу возможность безопасной цифровой идентификации человека в будущем. Стоит согласиться с И. А. Филиповой, обращающей внимание на актуализацию потребности в эффективной защите персональных данных работников в условиях цифровизации².

Уникальность биометрических персональных данных, их неотчуждаемость и невозможность изменения в случае компрометации обуславливают их особый правовой статус и повышенные риски для прав личности, что требует формирования адекватных правовых гарантий.

Российское законодательство и правоприменительная практика

Внедрение инвазивных технологий контроля и мониторинга исполнения трудовых обязанностей напрямую затрагивает конституционный принцип уважения человека труда (ст. 37 Конституции РФ³), который является составным элементом более общего принципа уважения прав человека. Последний предполагает признание достоинства личности (ст. 21 Конституции РФ) как универсальной ценности, представляющей собой незыблемый минимум, который должен гарантировать законодатель. Как подчеркивает М. В. Лушникова, «независимо от оценки данного человека обществом, его самооценки, каждый человек как личность имеет ценность в глазах государства и общества»⁴. Таким образом, принцип уважения человека

труда не допускает произвольного вмешательства государства и работодателя в сферу частной автономии личности трудящегося.

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»⁵ обработка биометрических персональных данных допускается только при наличии письменного согласия их субъекта. Указанное требование призвано устранить информационную асимметрию в отношениях между оператором и субъектом данных⁶.

Впрочем, на практике это правило подвергается эрозии за счет многочисленных нормативных исключений. Наиболее проблемной представляется «каучуковая» формулировка п. 2 ч. 1 ст. 6 Федерального закона от 27.07.2006 № 152-ФЗ, которая допускает обработку персональных данных без согласия субъекта, если она «необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей». Данная норма создает правовую основу для постоянного расширения перечня изъятий, позволяя отдельным категориям работодателей получать биометрические данные работников под угрозой применения дисциплинарных взысканий, вплоть до увольнения.

Подобная практика вызывает серьезные вопросы с точки зрения соблюдения статьи 9 Конвенции СНГ о правах и основных свободах человека (Минск, 26 мая 1995 г.)⁷, которая гарантирует каждому право на уважение его личной

² Филипова И. А. Трансформация правового регулирования труда в цифровом обществе. Искусственный интеллект и трудовое право : научное издание. Н. Новгород : Нижегородский государственный университет имени Н.И. Лобачевского, 2019. С. 16.

³ Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г., с изменениями, одобренными в ходе всероссийского голосования 1 июля 2020 г.) // Официальный интернет-портал правовой информации. URL: www.pravo.gov.ru. 06.10.2022.

⁴ Лушникова М. В. Сущность и природа прав работника на защиту достоинства, трудовой чести и деловой репутации // Вестник Пермского университета. Юридические науки. 2010. Вып. 1 (7). С. 34.

⁵ СЗ РФ. 2006. № 31 (ч. I). Ст. 3451.

⁶ Савельев А. И. Научно-практический комментарий к Федеральному закону «О персональных данных». М. : Статут, 2017. С. 71.

⁷ СЗ РФ. 1999. № 13. Ст. 1489.

жизни и допускает вмешательство государственных органов лишь в случаях, предусмотренных законом, и только когда это необходимо в демократическом обществе в интересах государственной безопасности или общественного порядка.

Яркой иллюстрацией сложившейся практики является дело № 8Г-8738/2023, рассмотренное Седьмым кассационным судом общей юрисдикции 25 июля 2023 г. Гражданин был уволен за прогул, который, по его мнению, произошел вследствие неправомерных действий службы охраны, не допустившей его на территорию АО «Нижевартовская ГРЭС» в связи с отказом пройти процедуру дактилоскопической регистрации. Локальным актом работодателя был установлен порядок, согласно которому проход на территорию разрешался исключительно при предъявлении пропуска и прохождении дактилоскопирования. Суды первой и кассационной инстанций отказали истцу в удовлетворении требований, поддержав позицию работодателя, который ссылаясь на установленные подзаконными актами требования антитеррористической защищенности объектов топливно-энергетического комплекса⁸.

Представляется, что подобные судебные решения⁹ носят спорный характер, поскольку суды, как правило, не исследуют ключевые вопросы соразмерности такого вмешательства. В частности, не оцениваются возможности использования работодателем альтернативных, менее инвазивных средств контроля доступа (электронные карты, бейджи) и исполнения трудовой функции за пределами особо охраняемого периметра. В этой связи уместно замечание Л. С. Таля: «Подчиняясь по трудовому договору хозяйской власти работодателя, работник не

отдает себя и свою рабочую силу на милость и усмотрение работодателю, а вправе ожидать, что предъявляемые ему требования и приказания не будут... посягать на неотчуждаемые личные блага и выходить из пределов тех задач предприятия, осуществлению которых работник обязался содействовать, одним словом — что хозяин будет пользоваться своей властью правомерно и целесообразно»¹⁰.

Дискуссионными являются и положения новейшего законодательства, легализующие сбор и передачу биометрических персональных данных без согласия их субъекта. Федеральный закон от 29.12.2022 № 572-ФЗ¹¹ устанавливает обязанность организаций и индивидуальных предпринимателей передавать в единую биометрическую систему (ЕБС) изображение лица и запись голоса человека, собранные с помощью технических средств, без получения на то согласия гражданина (ч. 14 ст. 4). Таким образом, если работник предоставил работодателю свои биометрические данные для внутренних нужд (например, для прохода в офис), работодатель, как следует из буквального толкования Закона, обязан принудительно и безвозмездно передать их в государственную систему. При этом данные в ЕБС сохраняются даже в случае прекращения их обработки первоначальным работодателем.

Фактически положения ч. 14 ст. 4 Федерального закона от 29.12.2022 № 572-ФЗ создают правовые условия для неконтролируемого со стороны гражданина вмешательства государства в сферу его частной автономии. Как справедливо отмечает А. А. Иванов, принятие этого Закона привело к «огосударствлению системы сбора, накопления и использования биометри-

⁸ Определение Судебной коллегии по гражданским делам Седьмого кассационного суда общей юрисдикции от 25.07.2023 по делу № 8Г-8738/2023[88-10266/2023] // СПС «Гарант».

⁹ См. также: определение Судебной коллегии по гражданским делам Седьмого кассационного суда общей юрисдикции от 09.06.2022 по делу № 8Г-7877/2022[88-9286/2022] ; решение Димитровградского городского суда Ульяновской области от 30.01.2023 по делу № 2-205/2023 // СПС «Гарант».

¹⁰ Таль Л. С. Трудовой договор : цивилистическое исследование. М. : Статут, 2006. С. 486.

¹¹ Федеральный закон от 29.12.2022 № 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» // СЗ РФ. 2023. № 1 (ч. I). Ст. 19.

ческих данных людей — наиболее чувствительной части персональных данных»¹². В этой связи обоснованными выглядят опасения некоторых исследователей о создании «условий для возвращения общества в кастовое прошлое и управление на основе страха и насилия государства над бесправной оцифрованной личностью»¹³. Эти риски в полной мере применимы и к сфере трудовых отношений, где современные информационные системы открывают работодателю возможности для установления гиперконтроля над работниками.

Сложившаяся ситуация вступает в очевидное противоречие с концепцией правового государства. Еще в 2000 г. в Послании Федеральному Собранию Президент РФ В. В. Путин указывал: «Наша важнейшая задача — научиться использовать инструменты государства для обеспечения свобод: свободы личности, свободы предпринимательства, свободы развития институтов гражданского общества»¹⁴.

Источником получения работодателем биометрической информации о работнике также являются видео- и аудиозаписи, которые могут быть использованы для мониторинга исполнения работниками трудовых обязанностей. Однако, как отмечает Е. В. Сыченко, отсутствие специального регулирования в трудовом законодательстве приводит к тому, что работники, оспаривающие решения работодателя, принятые по результатам видеонаблюдения, не ссылаются на незаконность соответствующих доказательств, а суды самостоятельно не исследуют факт законности видеозаписей¹⁵.

В связи с изложенным актуальным является вопрос не только о границах полномочий работодателя по принятию локальных нормативных актов, но и о пределах компетенции законодателя по ограничению права работника на его биометрические персональные данные. Представляется, что в России как правовом социальном государстве вмешательство в частную автономию личности возможно лишь при условии достижения справедливого баланса между публичными интересами и фундаментальными правами человека. Как минимум такое вмешательство должно быть соразмерно преследуемой законной цели¹⁶.

Страны ЕС

В Общем регламенте по защите данных ЕС¹⁷ (General Data Protection Regulation, GDPR) биометрические данные определяются как «персональные данные, полученные посредством определенной технической обработки, относящиеся к физическим, физиологическим или поведенческим характеристикам физического лица, которые позволяют или подтверждают его уникальную идентификацию, например изображения лица или данные отпечатков пальцев» (п. 14 ст. 4). В силу их тесной связи с человеческой сущностью и высокой чувствительности обработка биометрических данных запрещена (п. 1 ст. 9 GDPR). Как и в российском праве, из этого правила предусмотрены исключения, однако их применение, особенно в трудовых отно-

¹² Иванов А. А. Правовое регулирование биометрии в России: закон и практика // Вестник экономического правосудия Российской Федерации. 2024. № 11. С. 53.

¹³ Кашкин С. Ю., Покровский А. В. Искусственный интеллект, робототехника и защита прав человека в Европейском Союзе // Вестник Университета имени О.Е. Кутафина (МГЮА). 2019. № 4. С. 70.

¹⁴ Послание Федеральному Собранию Российской Федерации, 8 июля 2000 г., Москва, Кремль. С. 3 // Президент России : официальный сайт. URL: <https://www.prlib.ru/item/438199>.

¹⁵ Трудовое право: национальное и международное измерение : монография : в 2 т. / под ред. С. Ю. Головиной, Н. Л. Лютова. М. : Норма, 2022. Т. 1 : Общие проблемы современного трудового права. С. 300.

¹⁶ Дедов Д. И. Методология права 2.0. М. : Дело, 2023. С. 576.

¹⁷ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) // URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>.

шениях, строго регламентировано и основывается на ряде фундаментальных принципов¹⁸.

Принцип пропорциональности. Использование биометрических технологий работодателем должно быть строго пропорционально законной цели. Данный принцип также требует, чтобы при наличии нескольких одинаково эффективных мер выбиралась наименее обременительная для прав работника.

Пример. Испанское агентство по защите данных в одном из консультативных заключений признало допустимой обработку биометрических данных для системы доступа на объекты Национальной гвардии. Агентство указало на наличие объективного обоснования и конкретной необходимости внедрения такой системы, поскольку она обеспечивает более надежную, чем альтернативные механизмы, проверку лиц, имеющих доступ к защищенным зонам, и позволяет эффективно предотвращать несанкционированный доступ¹⁹.

Принцип минимизации данных. Обработка должна быть ограничена объемом информации, абсолютно необходимым для заявленной цели. Если работодателю требуется лишь зафиксировать факт присутствия сотрудника, сбор избыточных биометрических характеристик является незаконным. Как отмечают эксперты, «биометрический контроль доступа не должен становиться рутинным явлением в рамках организации, предприятия и без каких-либо оснований заменять другие существующие виды контроля, порой менее обременительные (бейдж, ключ, электронная карта и др.)»²⁰.

Пример. Итальянское управление по защите данных оштрафовало дилерский центр на 120 000 евро за использование системы распознавания лиц для контроля рабочего времени. Управление установило, что использование таких данных недопустимо, поскольку в Италии отсутствует закон, обязывающий применять биометрию для этих целей. Подчеркнуто, что даже согласие сотрудников не может служить правовым основанием для обработки данных ввиду системного дисбаланса власти в трудовых отношениях²¹.

Испанское агентство по защите данных допускает в исключительных случаях использование информационных систем контроля присутствия на рабочем месте, если такое использование полностью оправданно и законно, однако контролер, выбирая определенную биометрическую технологию для контроля присутствия работников, должен применять принцип минимизации данных (п. 1 ст. 25 GDPR). Для этого он обязан настроить систему контроля в соответствии с конкретными потребностями обработки и получить объективную оценку, результатом которой является отсутствие сбора избыточных данных для достижения цели обработки, в частности специальных категорий данных (ст. 35 GDPR)²².

Принцип прозрачности и информированного согласия. Для обработки биометрических данных требуется явное, информированное и специфическое согласие работника. Важно, что в контексте трудовых отношений добровольность такого согласия часто ставится под

¹⁸ Указанный ниже перечень не является исчерпывающим. Так, в ст. 5 GDPR закреплены семь основных принципов обработки персональных данных: законность, справедливость и прозрачность; ограничение цели; минимизация данных; точность; ограничение хранения; целостность и конфиденциальность; подотчетность.

¹⁹ ASUNTO: Consulta Previa (Art. 36 RGPD). Ref. REGAGE25e00024730156 // Agencia Española de Protección de Datos. URL: <https://www.aepd.es/documento/regage25e00024730156.pdf>.

²⁰ Рассолов И. М., Чубукова С. Г., Микурова И. В. Биометрия в контексте персональных данных и генетической информации: правовые проблемы // Lex russica. 2019. № 1. С. 111.

²¹ Garante privacy: riconoscimento facciale — no al controllo illecito delle presenze // Dottrina Per il Lavoro. 27 Giu 2024. URL: <https://www.dottrinalavoro.it/notizie-c/garante-privacy-riconoscimento-facciale-no-al-controllo-illecito-delle-presenze> (дата обращения: 09.11.2025).

²² Guía Tratamientos de control de presencia mediante sistemas biométricos. P. 8 // Agencia Española de Protección de Datos. URL: <https://www.aepd.es/guias/guia-control-presencia-biometrico.pdf> (дата обращения: 09.11.2025).

сомнение из-за зависимости работника от работодателя.

Пример. Испанская компания Plastic Forte, расположенная в Аликанте и специализирующаяся на сбыте пластиковой продукции, использовала распознавание лиц сотрудников для контроля за соблюдением рабочего времени и производительностью. При этом компания получила фотографии сотрудников под предлогом их использования в маркетинговых целях, не информируя о биометрической обработке. В результате Испанское агентство по защите данных наложило на компанию штраф в размере 12 000 евро²³.

Принцип безопасности данных. В соответствии со ст. 32 GDPR работодатель обязан принимать все необходимые технические и организационные меры для обеспечения безопасности биометрических данных. Это требование особенно критично, поскольку в отличие от паролей биометрию невозможно изменить после компрометации²⁴. Угрозы включают не только кибератаки на базы данных, но и использование технологий дипфейка (deepfake) для обмана биометрических систем²⁵.

Оценка воздействия на защиту данных (Data Protection Impact Assessment, DPIA) является ключевым процессуальным инструментом, обеспечивающим соблюдение вышеуказанных принципов (ст. 35 GDPR). Эта оценка проводится до начала обработки и направлена на выявление и минимизацию рисков для прав и свобод субъектов данных. Европейские регуляторы сформулировали детальные руководства по ее проведению²⁶.

Итальянское управление по защите данных привлекало работодателей к ответственности в числе прочего за непроведение DPIA в отношении систем отслеживания присутствия на рабочем месте²⁷. Французский регулятор (Commission nationale de l'informatique et des libertés, CNIL) уточняет, что в профессиональной среде допускается лишь биометрическая аутентификация на основе морфологических характеристик, в то время как сбор биологических образцов (слюны, крови) запрещен. Выбор конкретного типа биометрии работодателем должен быть обоснован и задокументирован, включая причину использования одного биометрического признака вместо другого²⁸.

В отличие от европейского подхода российское законодательство о персональных данных

²³ Resolución de terminación del procedimiento por pago voluntario : expediente N.º EXP202209921 // Agencia Española de Protección de Datos. URL: <https://www.supercontable.com/informacion/pdf/laboral/PS005972022.PDF> (дата обращения: 09.11.2025).

²⁴ Délibération n° 2015-087 du 5 mars 2015 refusant la mise en œuvre par la Banque Intesa Sanpaolo d'un traitement automatisé de données à caractère personnel reposant sur un dispositif biométrique de reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle et le suivi du temps de travail / Commission nationale de l'informatique et des libertés // URL: <https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000030481101/> (дата обращения: 09.11.2025).

²⁵ He S., Lei Y., Zhang Z., Sun Y., Li S., Zhang C., Ye J. Identity deepfake threats to biometric authentication systems: Public and expert perspectives // arXiv. June 7, 2025. URL: <https://arxiv.org/abs/2506.06825> (дата обращения: 09.11.2025).

²⁶ См., например: Gestión del riesgo y evaluación de impacto en tratamientos de datos personales // Agencia Española de Protección de Datos. URL: <https://www.aepd.es/guias/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf> (дата обращения: 09.11.2025).

²⁷ Garante privacy: no al riconoscimento facciale per il controllo delle presenze // Dottrina Per il Lavoro. 2 Apr 2024. URL: <https://www.dottrinalavoro.it/notizie-c/garante-privacy-no-al-riconoscimento-facciale-per-il-controllo-delle-presenze> (дата обращения: 09.11.2025).

²⁸ Délibération n° 2019-001 du 10 janvier 2019 portant règlement type relatif à la mise en œuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail // Commission nationale de l'informatique et des libertés. URL: <https://www.cnil.fr/sites/default/files/atoms/files/deliberation-2019-001-10-01-2019-reglement-type-controle-dacces-biometrique.pdf> (дата обращения: 09.11.2025).

устанавливает для операторов лишь общее требование по оценке вреда, который может быть причинен субъектам, но не предусматривает обязательной, структурированной и документированной процедуры оценки воздействия до начала обработки. Такой пробел в регулировании лишает правоприменительную практику важного инструмента, позволяющего взвесить необходимость и соразмерность вмешательства в частную сферу работника.

Выводы

Использование биометрических данных, безусловно, может быть мощным инструментом повышения эффективности и безопасности бизнеса. Однако оно создает значительные риски для личных неимущественных прав работников, требуя адекватного правового противовеса. Внедрение таких технологий без должных гарантий не соответствует принципам уважения человека труда и охраны человеческого достоинства. Трудовое право нуждается в развитии норм, ограничивающих возможности работодателей по использованию цифровых технологий.

Проведенный анализ демонстрирует существенные различия в подходах к регулированию обработки биометрических данных работников в России и ЕС. Российская модель, формально провозглашая приоритет согласия, на практике до-

пускает широкие исключения, оправдываемые ссылками на государственные и корпоративные интересы, без надлежащей проверки их соразмерности. Европейская модель, основанная на GDPR, создает более сбалансированный режим.

В целях совершенствования российского законодательства и правоприменительной практики целесообразно:

1) ввести требование проводить оценку воздействия на защиту персональных данных (по аналогии со ст. 35 GDPR) как подзаконных, так и локальных нормативных актов, которые предусматривают внедрение (требуют внедрения) систем, связанных с обработкой биометрических и иных специальных категорий данных;

2) разработать и утвердить на уровне Роскомнадзора конкретные руководства и методические рекомендации для работодателей по управлению рисками и проведению оценки воздействия с учетом отраслевой специфики;

3) на уровне постановления Пленума Верховного Суда РФ стимулировать суды к более тщательной проверке соразмерности вмешательства в частную жизнь работников, в том числе к оценке наличия у работодателя менее инвазивных альтернатив достижения заявленных легитимных целей.

Внедрение подобных гарантий позволит достичь более справедливого баланса интересов работодателей, государства и личности в цифровую эпоху.

БИБЛИОГРАФИЯ

1. Дедов Д. И. Методология права 2.0. — М. : Дело, 2023. — 750 с.
2. Иванов А. А. Правовое регулирование биометрии в России: закон и практика // Вестник экономического правосудия Российской Федерации. — 2024. — № 11. — С. 52–62.
3. Кашкин С. Ю., Покровский А. В. Искусственный интеллект, робототехника и защита прав человека в Европейском Союзе // Вестник Университета имени О.Е. Кутафина (МГЮА). — 2019. — № 4. — С. 64–90.
4. Лушникова М. В. Сущность и природа прав работника на защиту достоинства, трудовой чести и деловой репутации // Вестник Пермского университета. Юридические науки. — 2010. — Вып. 1 (7). — С. 32–37.
5. Рассолов И. М., Чубукова С. Г., Микурова И. В. Биометрия в контексте персональных данных и генетической информации: правовые проблемы // Lex russica. — 2019. — № 1. — С. 108–118.
6. Савельев А. И. Научно-практический комментарий к Федеральному закону «О персональных данных». — М. : Статут, 2017. — 317 с.
7. Таль Л. С. Трудовой договор : цивилистическое исследование. — М. : Статут, 2006.

8. Трудовое право: национальное и международное измерение : монография : в 2 т. Т. 1 : Общие проблемы современного трудового права / под ред. С. Ю. Головиной, Н. Л. Лютова. — М. : Норма, 2022. — 608 с.
9. Филипова И. А. Трансформация правового регулирования труда в цифровом обществе. Искусственный интеллект и трудовое право : научное издание. — Н. Новгород : Нижегородский государственный университет имени Н.И. Лобачевского, 2019. — 89 с.
10. He S., Lei Y., Zhang Z., Sun Y., Li S., Zhang C., Ye J. Identity deepfake threats to biometric authentication systems: Public and expert perspectives // arXiv. — June 7, 2025. — URL: <https://arxiv.org/abs/2506.06825>.
11. Person identification, human rights and ethical principles: Rethinking biometrics in the era of artificial intelligence (PE 697.191, December 2021) / European Parliamentary Research Service ; Scientific Foresight Unit. — European Union, 2021.

Материал поступил в редакцию 18 ноября 2025 г.

REFERENCES (TRANSLITERATION)

1. Dedov D. I. Metodologiya prava 2.0. — М.: Delo, 2023. — 750 s.
2. Ivanov A. A. Pravovoe regulirovanie biometrii v Rossii: zakon i praktika // Vestnik ekonomicheskogo pravosudiya Rossiyskoy Federatsii. — 2024. — № 11. — S. 52–62.
3. Kashkin S. Yu., Pokrovskiy A. V. Iskusstvennyy intellekt, robototekhnika i zashchita prav cheloveka v Evropeyskom Soyuze // Vestnik Universiteta imeni O.E. Kutafina (MGYuA). — 2019. — № 4. — S. 64–90.
4. Lushnikova M. V. Sushchnost i priroda prav rabotnika na zashchitu dostoinstva, trudovoy chesti i delovoy reputatsii // Vestnik Permskogo universiteta. Yuridicheskie nauki. — 2010. — Vyp. 1 (7). — S. 32–37.
5. Rassolov I. M., Chubukova S. G., Mikurova I. V. Biometriya v kontekste personalnykh dannykh i geneticheskoy informatsii: pravovye problemy // Lex russica. — 2019. — № 1. — S. 108–118.
6. Savelev A. I. Nauchno-prakticheskiy kommentariy k Federalnomu zakonu «O personalnykh dannykh». — М.: Statut, 2017. — 317 s.
7. Tal L. S. Trudovoy dogovor: tsivilisticheskoe issledovanie. — М.: Statut, 2006.
8. Трудовое право: национальное и международное измерение: монография: в 2 т. Т. 1: Общие проблемы современного трудового права / под ред. С. Ю. Головиной, Н. Л. Лютова. — М.: Норма, 2022. — 608 с.
9. Filipova I. A. Transformatsiya pravovogo regulirovaniya truda v tsifrovom obshchestve. Iskusstvennyy intellekt i трудовое право: nauchnoe izdanie. — N. Novgorod: Nizhegorodskiy gosudarstvennyy universitet imeni N.I. Lobachevskogo, 2019. — 89 s.
10. He S., Lei Y., Zhang Z., Sun Y., Li S., Zhang C., Ye J. Identity deepfake threats to biometric authentication systems: Public and expert perspectives // arXiv. — June 7, 2025. — URL: <https://arxiv.org/abs/2506.06825>.
11. Person identification, human rights and ethical principles: Rethinking biometrics in the era of artificial intelligence (PE 697.191, December 2021) / European Parliamentary Research Service; Scientific Foresight Unit. — European Union, 2021.