

ПРЕОБРАЗОВАНИЕ ИНСТИТУТА ПРАВОВОЙ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЭПОХУ ВНЕДРЕНИЯ БИОМЕТРИЧЕСКИХ ТЕХНОЛОГИЙ

НОСЕНКО Л.И. 

Носенко Лидия Ивановна – Кандидат юридических наук, заведующий кафедрой Гражданского права и процесса юридического факультета, Оренбургский государственный университет имени В.А. Бондаренко, г. Оренбург, Российская Федерация

E-mail: lidiano@list.ru, <https://orcid.org/0000-0001-9909-2301>

Аннотация. В научной статье исследуется процесс трансформации правового института защиты персональных данных в условиях стремительного развития и внедрения биометрических технологий. Автор анализирует специфику биометрических персональных данных как особой, высокочувствительной категории информации, обладающей фундаментальными свойствами неотчуждаемости и неизменяемости. Эти уникальные характеристики предопределяют возникновение повышенных рисков для конфиденциальности, цифровой идентичности и общей безопасности субъектов правоотношений. В работе детально рассматриваются актуальные изменения в национальном и международном законодательстве, выявляются существенные пробелы в существующем нормативно-правовом регулировании и правоприменительной практике. Особое внимание уделено поиску справедливого баланса между государственными интересами в сфере безопасности, коммерческой целесообразностью бизнеса и фундаментальными конституционными правами человека на неприкосновенность частной жизни. На основе глубокого сравнительно-правового анализа автором предложены комплексные рекомендации по совершенствованию нормативно-правовой базы. Они включают в себя ужесточение юридической ответственности за неправомерный оборот и утечку биометрии, внедрение механизмов обязательного предварительного аудита систем распознавания, а также законодательное закрепление международной концепции «проектируемой конфиденциальности». Представленная научная статья ориентирована на практикующих юристов и специалистов в области информационной безопасности.

Ключевые слова: персональные данные, биометрические технологии, правовая защита, конфиденциальность, цифровая трансформация, искусственный интеллект, информационная безопасность.

Введение

Эпоха промышленной революции ознаменовалась глубокой интеграцией цифровых технологий во все сферы общественной и государственной жизни. Среди множества инновационных инструментов особое место заняли биометрические технологии, обеспечивающие идентификацию и аутентификацию человека на основе его уникальных физиологических и поведенческих характеристик. Сегодня распознавание лиц, сканирование отпечатков пальцев, радужной оболочки глаз, анализ голоса и походки активно применяются не только в сфере обеспечения национальной безопасности и криминалистики, но и в повседневной коммерческой практике: от банковского обслуживания и ритейла до систем контроля доступа на рабочие места.

Стремительное, повсеместное внедрение биометрии порождает фундаментальные вызовы для традиционного института правовой защиты персональных данных. В отличие от классических идентификаторов (паспортные данные, пароли, адреса электронной почты), биометрические данные неразрывно связаны с физическим телом человека. Их невозможно изменить в случае компрометации или утечки. Утечка биометрического шаблона означает безвозвратную потерю контроля над цифровой идентичностью гражданина, что открывает беспрецедентные возможности для мошенничества, тотальной слежки и несанкционированного профилирования.

Целью научной статьи является комплексное теоретико-правовое исследование процесса трансформации института правовой защиты персональных данных под влиянием повсеместного внедрения биометрических технологий, а также выработка научно обоснованных рекомендаций по совершенствованию законодательства для эффективного баланса между технологическим прогрессом и защитой фундаментальных прав человека на неприкосновенность частной жизни. Для достижения этой цели в научной статье решаются

следующие задачи:

1. Определение юридической природы и специфики биометрических данных в цифровую эпоху.
2. Выявление ключевых правовых рисков и угроз, возникающих при массовом использовании систем распознавания.
3. Сравнительно-правовой анализ международного опыта (GDPR, AI Act) и российского законодательства (ФЗ № 152, ФЗ № 572).
4. Формулирование концептуальных изменений для нормативно-правовой базы (внедрение принципов Privacy by Design, регулирование поведенческой биометрии, усиление ответственности операторов).

Материалы и методы исследования

Методологическую основу исследования составляют комплекс общенаучных и специальных методов, материалами исследования служат международные акты, российское законодательство, судебная практика и научная доктрина. Для анализа применяются сравнительно-правовой, формально-юридический, системно-структурный и прогностический методы. В статье применяется сравнительно-правовой метод для сопоставления норм GDPR, AI Act и российского ФЗ № 572, а также формально-юридический метод для анализа понятия биометрических данных. Применен системно-структурный подход для оценки трансформации смежных правовых институтов и метод правового прогнозирования для моделирования векторов развития законодательства в сфере биометрии.

Результаты и их обсуждение

В статье рассматривается и теоретико-правовая сущность биометрических персональных данных. Для понимания масштаба трансформации правового института необходимо четко определить юридическую природу биометрических персональных данных. В соответствии с доктриной информационного права, под биометрическими данными понимаются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.

Основная специфика биометрии заключается в ее дуалистической природе. С одной стороны, это объективная биологическая информация, присущая индивиду с рождения. С другой стороны, в правовом поле она становится персональными данными только тогда, когда используется оператором именно для установления личности.

В условиях применения технологий искусственного интеллекта и машинного обучения традиционная граница между общими и биометрическими данными стремительно размывается. Современные нейросети способны извлекать биометрические маркеры из видеопотока низкого разрешения или по косвенным признакам (манера набора текста, особенности микроподвижности рук). Это требует переосмысления классических подходов к категоризации информации.

Необходимо затронуть и вопрос рисков и угроз прав человека в условиях биометризации. Массовый сбор и централизованное хранение биометрической информации формируют новые типы правовых и социальных рисков:

1. Риск необратимой компрометации - невозможность смены биометрического ключа в случае утечки базы данных.
2. Угроза приватности в публичном пространстве из-за систем распознавания лиц в реальном времени.
3. Функциональное распространение (Function Creep) - использование данных, собранных для одной цели, в коммерческих или иных негласных целях.
4. Дискриминация и алгоритмические ошибки - погрешности работы нейросетей в отношении отдельных социальных групп.

Хотелось бы обратить внимание на трансформацию нормативно-правового регулирования и провести анализ международного и национального опыта. Глобальным стандартом выступает Общий регламент по защите данных Европейского Союза (GDPR), который относит биометрические данные к специальным категориям, и принятый Акт об

искусственном интеллекте (AI Act), накладывающий жесткие запреты на биометрическую идентификацию в реальном времени. В Российской Федерации ключевым этапом стало принятие Федерального закона № 572-ФЗ, упорядочившего сбор биометрии через Единую биометрическую систему (ЕБС) и закрепившего право граждан на отказ от сбора биометрических данных [1].

Глобальный вектор правовой трансформации в сфере биометрии задается наднациональным законодательством Европейского Союза, которое демонстрирует последовательный переход от базовой защиты конфиденциальности к жесткому ограничению применения сквозных цифровых технологий. До недавнего времени фундаментом регулирования выступал Общий регламент по защите данных (GDPR). В соответствии со ст. 9 GDPR, биометрические данные отнесены к специальным категориям («чувствительным» данным), обработка которых по общему правилу запрещена, за исключением случаев получения явного (explicit) согласия субъекта или защиты жизненно важных интересов. Однако практика показала, что модель «информированного согласия» в условиях цифровых платформ не способна полностью защитить граждан от скрытого профилирования.

Качественным сдвигом в международной практике стало принятие и вступление в силу Акта об искусственном интеллекте Европейского Союза (EU AI Act/ Регламент ЕС 2024/1689), положения которого поэтапно разворачиваются в 2025-2026 годах. Данный документ внедряет риск-ориентированный подход, разделяя ИИ-системы на уровни угрозы:

1. Неприемлемый риск (Unacceptable Risk): С февраля 2025 года введен полный запрет на использование систем распознавания эмоций (Emotion Recognition) на рабочих местах и в образовательных учреждениях, а также систем биометрической категоризации людей по расовым, политическим или религиозным признакам. Использование удаленной биометрической идентификации (RBI) в реальном времени в общественных местах для целей правоохранительных органов запрещено (за исключением расследования строго ограниченного круга тяжких преступлений и поиска пропавших лиц).

2. Высокий риск (High-Risk): Системы биометрической аутентификации, контроля доступа и верификации идентичности отнесены к категории высокого риска. К ним применяются жесткие требования по обеспечению качества обучающих датасетов, непрерывному человеческому надзору (human oversight) и обязательной регистрации в общеевропейской базе данных.

Правоприменительная практика ЕС подкреплена беспрецедентным штрафным режимом: за нарушение запретов в сфере биометрии предусмотрены административные взыскания до 35 миллионов евро или до 7% от годового глобального оборота компании [2].

Российская модель правового регулирования биометрических технологий пошла по пути жесткой централизации и создания государственного монополиста в области хранения биометрических шаблонов, что принципиально отличает ее от децентрализованного европейского подхода.

Ключевым элементом национальной нормативной базы выступает Федеральный закон № 572-ФЗ. Этот закон радикально изменил ландшафт применения биометрических технологий в коммерческом секторе и государственном управлении, разделив обработку данных на два режима:

1. Централизованный контур (Единая биометрическая система - ЕБС): Закон установил императивное правило - коммерческие организации (банки, ритейл, операторы связи) не имеют права хранить в своих локальных базах данных «сырые» биометрические образцы (фотографии лица, записи голоса) для целей автоматизированной идентификации. Все ранее собранные коммерческими структурами биометрические данные подлежали обязательной передаче в ЕБС.

2. Локальный контур (Векторный режим): Организациям разрешено использовать биометрию в локальных системах контроля и управления доступом (СКУД) на предприятиях или для авторизации на устройствах (Face ID на проходной) в виде зашифрованных математических векторов (хэш-шаблонов), которые невозможно деконструировать обратно в

изображение лица, либо путем прямой интеграции оборудования с аккредитованными сегментами ЕБС.

Законодатель существенно усилил гарантии прав граждан. Согласно ст. 3 закона № 572-ФЗ, предоставление биометрии является исключительно добровольным, а отказ гражданина от сдачи биометрических данных не может служить основанием для отказа в предоставлении государственных или муниципальных услуг, а также в коммерческом обслуживании. Гражданин получил право в любой момент отозвать свое согласие или полностью удалить свои биометрические данные из ЕБС через портал «Госуслуги».

Эволюция российского законодательства выразилась также в ужесточении ответственности за неправомерную обработку. В соответствии с поправками (ФЗ № 420-ФЗ), административные штрафы за незаконный сбор, обработку или хранение биометрии без согласия субъекта были увеличены до 2 миллионов рублей для юридических лиц, что сделало нарушение требований ФЗ № 572-ФЗ экономически критичным для бизнеса [3; 4].

Процессы нормативной трансформации активно затронули и другие страны постсоветского пространства [5]. Характерным примером является Республика Казахстан, где правовое регулирование биометрии также движется в сторону императивного внедрения государственных верификационных сервисов для минимизации кибермошенничества и предотвращения незаконного оборота персональных данных [6].

В 2025-2026 годах Министерство искусственного интеллекта и цифрового развития РК инициировало масштабные изменения в правила регистрации мобильных устройств и оказания услуг связи. Согласно новым требованиям, первичная регистрация абонентских устройств (по IMEI-кодам) и заключение договоров сотовой связи требуют обязательной биометрической аутентификации заявителя с последующим автоматизированным сопоставлением данных с государственными базами [7; 8]. Этот опыт демонстрирует государственную тенденцию признания биометрии единственным надежным юридическим инструментом верификации цифровой идентичности гражданина, несмотря на сопутствующие риски централизации.

Международный и национальный опыт демонстрирует две противоположные, но одинаково радикальные стратегии адаптации права к вызовам биометрии: европейскую стратегию «запретительно-ограничительного шлюза» и российскую стратегию «государственного сейфа» [9; 10]. Обе модели направлены на изъятие биометрических массивов из неконтролируемого коммерческого оборота, однако они требуют постоянного мониторинга на предмет соблюдения баланса между публичной безопасностью и правами личности.

Необходимо выделить пути совершенствования института правовой защиты биометрических данных:

1. Внедрение концепции «проектируемой конфиденциальности» (Privacy by Design).
2. Законодательное признание и регулирование поведенческой биометрии.
3. Ужесточение юридической ответственности операторов и введение оборотных штрафов.
4. Установление жестких рамок для государственного использования биометрии под судебным контролем.

Заключение

Трансформация права должна идти по пути перехода от декларативной защиты к технологически подкрепленным правовым барьерам.

Традиционная модель регулирования персональных данных, опирающаяся исключительно на постфактумное выявление нарушений и бумажное администрирование («информированные согласия»), окончательно исчерпала себя в условиях тотальной биометризации и применения сквозных систем искусственного интеллекта. Будущее правового института защиты конфиденциальности лежит в плоскости конвергенции юридических норм и программно-аппаратных алгоритмов.

Проведенное исследование позволяет сформулировать следующие концептуальные

выводы и направления реформирования отрасли:

1. Переход к концепции «Проектируемой конфиденциальности» (Privacy by Design): Нормативно-правовые акты нового поколения должны обязывать разработчиков биометрических систем внедрять защитные механизмы (сквозное шифрование, локальное хэширование, автоматическое обезличивание) непосредственно на этапе проектирования архитектуры программного обеспечения, а не надстраивать их поверх готовых решений.

2. Синхронизация правовых и технологических стандартов: Юридическая ответственность операторов обязана соотноситься с жесткими ИТ-стандартами. Государственный контроль должен быть смещен с формальной проверки документов на обязательный независимый аудит алгоритмов распознавания. Это необходимо для предотвращения скрытого «расползания функций» (Function Creep) и минимизации рисков дискриминации граждан из-за ошибок нейросетей.

3. Императивное разграничение публичных и частных интересов: Международный опыт (в частности, EU AI Act) и эволюция национального законодательства (ФЗ № 572-ФЗ) наглядно демонстрируют, что бесконтрольный оборот биометрических шаблонов в коммерческом секторе несет критическую угрозу национальной безопасности и правам личности. Необходима дальнейшая минимизация присутствия частных компаний в процессах первичного сбора и хранения «сырых» биометрических данных.

4. Опережающее регулирование новых форм биометрии: Современное право обязано оперативно реагировать на появление технологий распознавания поведенческой биометрии (походка, микродинамика, паттерны взаимодействия с интерфейсами) и систем ИИ-анализа эмоций. Введение превентивных законодательных ограничений на их использование в коммерческих целях, трудовых и образовательных отношениях является важнейшей задачей правотворца на среднесрочную перспективу.

Только жесткий правовой каркас, сочетающий строгую ответственность операторов, технологические стандарты безопасности и безусловный приоритет прав человека, позволит минимизировать риски цифровой эпохи. Государствам предстоит пройти сложный путь от простого фиксирования фактов утечек к созданию проактивной цифровой правовой среды. В этой среде право выступает не тормозом технологического прогресса, а гарантией того, что данный прогресс направлен на благо человека, сохранение его автономии, достоинства и фундаментального права на неприкосновенность частной жизни.

Список литературы

1. 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 : Федеральный закон от 29 декабря 2022 г. № 572-ФЗ [Электронный ресурс] // Официальное опубликование правовых актов. — URL: <https://publication.pravo.gov.ru/Document/View/0001202212290024>

2. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ: с изменениями и дополнениями [Электронный ресурс] // Собрание законодательства Российской Федерации. — 2006. — № 31, ч. 1. — Ст. 3448.

3. О внесении изменений в Кодекс Российской Федерации об административных правонарушениях: Федеральный закон от 30 ноября 2024 г. № 420-ФЗ [Электронный ресурс] // Официальное опубликование правовых актов. — URL: <https://publication.pravo.gov.ru/Document/View/0001202411300011>

4. Кодекс Российской Федерации об административных правонарушениях: Федеральный закон от 30 декабря 2001 г. № 195-ФЗ: с изменениями и дополнениями. — Ст. 13.11 // Собрание законодательства Российской Федерации. — 2002. — № 1, ч. 1. — Ст. 1.

5. Амелин Р. В., Великородная Л. И. Правовое регулирование обращения биометрических персональных данных: мировой опыт и российские реалии //

Информационное право. - 2023. - № 2. - С. 18-24.

6. Жарова А. К. Защита персональных данных в условиях применения технологий искусственного интеллекта // Бизнес-информатика. - 2023. - Т. 17. - № 1. - С. 62-74.

7. Ковалева Н. Н. Трансформация правового статуса субъекта персональных данных в цифровую эпоху. // Вестник Саратовской государственной юридической академии. - 2024. - № 1. - С. 112-120.

8. Минбалеев А. В. Проблемы правового регулирования использования биометрических персональных данных в Российской Федерации // Вестник ЮУрГУ. Серия: Право. - 2023. - Т. 23. - № 3. - С. 75-81.

9. Полякова Т. А., Стрельцов А. А. Международно-правовые стандарты защиты прав человека в информационной сфере и тенденции их развития. // Труды Института государства и права РАН. - 2022. - Т. 17. - № 5.- С. 34-52.

10. Рассолов И. М., Чубукова С. Г. Биометрические данные в фокусе права: от идентификации к цифровому профилированию. // Lex Russica. - 2024. - № 2. - С. 58-71.

References

1. Ob osushchestvlenii identifikatsii i (ili) autentifikatsii fizicheskikh lic s ispol'zovaniem biometricheskikh personal'nykh dannykh, o vnesenii izmenenij v otdel'nye zakonodatel'nye akty Rossijskoj Federatsii i priznanii utrativshimi silu otdel'nykh polozhenij zakonodatel'nykh aktov Rossijskoj Federatsii : Federal'nyj zakon ot 29 dekabrya 2022 g. № 572-FZ [Elektronnyj resurs] // Oficial'noe opublikovanie pravovykh aktov. — URL: <https://publication.pravo.gov.ru/Document/View/0001202212290024>

2. Ob informatsii, informatsionnykh tekhnologiyah i o zashchite informatsii: Federal'nyj zakon ot 27 iyulya 2006 g. № 149-FZ: s izmeneniyami i dopolneniyami [Elektronnyj resurs] // Sobranie zakonodatel'stva Rossijskoj Federatsii. — 2006. — № 31, ch. 1. — St. 3448.

3. O vnesenii izmenenij v Kodeks Rossijskoj Federatsii ob administrativnykh pravonarusheniyah: Federal'nyj zakon ot 30 noyabrya 2024 g. № 420-FZ [Elektronnyj resurs] // Oficial'noe opublikovanie pravovykh aktov. — URL: <https://publication.pravo.gov.ru/Document/View/0001202411300011>

4. Kodeks Rossijskoj Federatsii ob administrativnykh pravonarusheniyah: Federal'nyj zakon ot 30 dekabrya 2001 g. № 195-FZ: s izmeneniyami i dopolneniyami. — St. 13.11 // Sobranie zakonodatel'stva Rossijskoj Federatsii. — 2002. — № 1, ch. 1. — St. 1.

5. Amelin R. V., Velikorodnaya L. I. Pravovoe regulirovanie obrashcheniya biometricheskikh personal'nykh dannykh: mirovoj opyt i rossijskie realii // Informatsionnoe pravo. - 2023. - № 2. - S. 18-24.

6. ZHarova A. K. Zashchita personal'nykh dannykh v usloviyakh primeneniya tekhnologij iskusstvennogo intellekta // Biznes-informatika. - 2023. - Т. 17. - № 1. - S. 62-74.

7. Kovaleva N. N. Transformatsiya pravovogo statusa sub"ekta personal'nykh dannykh v cifrovuyu epohu. // Vestnik Saratovskoy gosudarstvennoy yuridicheskoy akademii. - 2024. - № 1. - S. 112-120.

8. Minbaleev A. V. Problemy pravovogo regulirovaniya ispol'zovaniya biometricheskikh personal'nykh dannykh v Rossijskoj Federatsii // Vestnik YUUrGU. Seriya: Pravo. - 2023. - Т. 23. - № 3. - S. 75-81.

9. Polyakova T. A., Strel'cov A. A. Mezhdunarodno-pravovye standarty zashchity prav cheloveka v informatsionnoj sfere i tendentsii ih razvitiya. // Trudy Instituta gosudarstva i prava RAN. - 2022. - Т. 17. - № 5.- S. 34-52.

10. Rassolov I. M., CHubukova S. G. Biometricheskie dannye v fokuse prava: ot identifikatsii k cifrovomu profilirovaniyu. // Lex Russica. - 2024. - № 2. - S. 58-71.

НОСЕНКО Л.И. 

Носенко Лидия Ивановна - Заң ғылымдарының кандидаты, заң факультетінің Азаматтық құқық және процесс кафедрасының меңгерушісі, В.А. Бондаренко атындағы Орынбор мемлекеттік университеті, Орынбор қ., Ресей Федерациясы

E-mail: lidiano@list.ru, <https://orcid.org/0000-0001-9909-2301>

Аңдатпа. Ғылыми мақалада қарқынды даму және биометриялық технологияларды енгізу жағдайында дербес деректерді қорғау құқықтық институтын трансформациялау процесі зерттеледі. Автор биометриялық дербес деректердің ерекшелігін иеліктен шығарылмайтын және өзгермейтін негізгі қасиеттері бар ақпараттың ерекше, жоғары сезімтал категориясы ретінде талдайды. Бұл бірегей сипаттамалар құпиялылық, цифрлық сәйкестік және құқықтық қатынастар субъектілерінің жалпы қауіпсіздігі үшін жоғары тәуекелдердің пайда болуын алдын ала анықтайды. Жұмыста ұлттық және халықаралық заңнамадағы өзекті өзгерістер егжей-тегжейлі қарастырылады, қолданыстағы нормативтік-құқықтық реттеу мен құқық қолдану практикасындағы елеулі олқылықтар анықталады. Қауіпсіздік саласындағы мемлекеттік мүдделер, бизнестің коммерциялық орындылығы және адамның жеке өмірге қол сұғылмаушылыққа негізгі конституциялық құқықтары арасындағы әділ теңгерімді іздеуге ерекше назар аударылады. Терең салыстырмалы-құқықтық талдау негізінде автор нормативтік-құқықтық базаны жетілдіру бойынша кешенді ұсыныстар ұсынды. Олар заңсыз айналым мен биометрияның ағуы үшін заңды жауапкершілікті қатаңдату, тану жүйелеріне міндетті алдын ала аудит жүргізу тетіктерін енгізуді, сондай-ақ «жобаланған құпиялылық» халықаралық тұжырымдамасын заңнамалық тұрғыдан бекітуді қамтиды. Ұсынылған ғылыми мақала Ақпараттық қауіпсіздік саласындағы тәжірибелі заңгерлер мен мамандарға бағытталған.

Түйін сөздер: дербес деректер, биометриялық технологиялар, құқықтық қорғау, құпиялылық, цифрлық трансформация, жасанды интеллект, ақпараттық қауіпсіздік.

TRANSFORMATION OF THE INSTITUTE OF LEGAL PROTECTION OF PERSONAL DATA IN THE ERA OF THE INTRODUCTION OF BIOMETRIC TECHNOLOGIES

NOSENKO L.I. 

Nosenko Lidiya Ivanovna - Candidate of law, Head of the department of civil law and procedure, Orenburg state university named after V.A. Bondarenko, Orenburg, Russian Federation

E-mail: lidiano@list.ru, <https://orcid.org/0000-0001-9909-2301>

Abstract. The scientific article examines the process of transformation of the legal institution of personal data protection in the context of the rapid development and implementation of biometric technologies. The author analyzes the specifics of biometric personal data as a special, highly sensitive category of information with fundamental properties of inviolability and immutability. These unique characteristics determine the emergence of increased risks to privacy, digital identity, and the overall security of legal entities. The paper examines in detail current changes in national and international legislation, identifies significant gaps in existing legal regulation and law enforcement practice. Special attention is paid to the search for a fair balance between state interests in the field of security, commercial expediency of business and fundamental constitutional human rights to privacy. Based on an in-depth comparative legal analysis, the author offers comprehensive recommendations for improving the regulatory framework. These include stricter legal liability for the illegal turnover and leakage of biometrics, the introduction of mandatory pre-audit mechanisms for recognition systems, as well as the legislative consolidation of the international concept of «projected privacy». The presented scientific article is aimed at practicing lawyers and specialists in the field of information security.

Key words: personal data, biometric technologies, legal protection, confidentiality, digital transformation, artificial intelligence, information security.