

ОСОБЫЙ ПРАВОВОЙ РЕЖИМ И ГАРАНТИИ ОБРАБОТКИ БИОМЕТРИЧЕСКИХ ДАННЫХ В УЗБЕКИСТАНЕ

Иброхимова Назирахон Илхомжлн кизи

Магистрант Ташкентского государственного юридического университета
направление бизнес право.

<https://doi.org/10.5281/zenodo.20543036>

Аннотация. Настоящий тезис посвящён комплексному исследованию правового режима биометрических данных в Республике Узбекистан. В работе анализируются нормативная база, существующие законодательные пробелы, механизмы гарантий защиты прав субъектов персональных данных, а также международный опыт регулирования биометрической информации. На основе сравнительно-правового метода выявлены системные проблемы действующего регулирования и сформулированы конкретные предложения по его совершенствованию в контексте цифровой трансформации Узбекистана.

Ключевые слова: биометрические данные, персональные данные, правовой режим, локализация данных, согласие субъекта, информационная безопасность, надзор, GDPR, цифровые права, Узбекистан.

В эпоху повсеместной цифровизации биометрические технологии стремительно вошли в повседневную жизнь: системы распознавания лиц открывают двери офисов и аэропортов, сканеры отпечатков пальцев заменяют банковские карты, а голосовые идентификаторы подтверждают личность клиентов финансовых организаций.

В отличие от пароля, номера документа или PIN-кода биометрические данные — это не условный знак, присвоенный человеку извне, а неотъемлемая часть его физической личности. Они неизменяемы, неотчуждаемы и уникальны.

Именно эти свойства делают биометрическую информацию исключительно ценным идентификатором, а одновременно — исключительно опасным объектом в случае её утечки или злоупотребления: в отличие от утраченного пароля, скомпрометированный биометрический шаблон не может быть заменён.

Республика Узбекистан активно движется по пути цифровой трансформации.

Национальная стратегия «Цифровой Узбекистан — 2030» предусматривает масштабное внедрение биометрических технологий в систему государственного управления, здравоохранение, финансовый сектор и образование. Биометрические данные уже сегодня собираются при оформлении удостоверений личности, при открытии банковских счетов, при регистрации на государственных порталах и в системах контроля доступа. По данным экспертов правового клиника Узбекистана, биометрические системы применяются в правоохранительной деятельности для дактилоскопического учёта, а в банковском секторе — для идентификации клиентов по лицу и голосу в режиме реального времени.

Столь широкое применение биометрических технологий ставит перед государством принципиальный вопрос: соответствует ли правовой режим обработки таких данных их особой природе и степени риска для граждан?

Проведённый анализ показывает, что ответ на этот вопрос остаётся во многом отрицательным. Несмотря на определённый прогресс последних лет, законодательство Узбекистана в данной сфере характеризуется существенными системными пробелами: отсутствием специального закона, декларативностью действующих норм, запоздалым введением технических стандартов и механизмов реальной ответственности операторов.

Тезис настоящей работы формулируется следующим образом: правовой режим биометрических данных в Узбекистане, хотя и закреплён в общих чертах в Законе «О персональных данных» 2019 года, не образует достаточной системы гарантий защиты прав субъектов, поскольку лишён специального нормативного регулирования, действенных механизмов надзора, требований прозрачности алгоритмов и соразмерной юридической ответственности, что делает необходимым комплексное реформирование в данной сфере.

Цель настоящего тезиса — на основе анализа действующего законодательства, правоприменительной практики и зарубежного опыта выявить ключевые проблемы правового регулирования биометрических данных в Узбекистане и сформулировать научно обоснованные предложения по его совершенствованию. Методологической основой работы служат формально-юридический, сравнительно-правовой и системный методы исследования.

Правовое регулирование биометрических данных в Узбекистане осуществляется в рамках общего законодательства о персональных данных. Фундаментом служит Закон Республики Узбекистан «О персональных данных» № ЗРУ-547, принятый 2 июля 2019 года и впоследствии неоднократно дополнявшийся. Закон определяет биометрические данные как самостоятельную категорию, требующую особого подхода, и посвящает их регулированию статью 26, которая устанавливает, что обработка биометрических и генетических данных в целях идентификации личности допускается только при наличии письменного согласия субъекта. Исключения предусмотрены для случаев правосудия, исполнительного производства и реализации международных договоров.

Дополнительное регулирование в данной сфере осуществляется Постановлением Кабинета Министров № 2 от 2023 года, которым установлены конкретные технические требования к хранению биометрических и генетических данных: при электронном хранении такие данные подлежат обязательному криптографическому шифрованию; владелец и оператор базы данных несут ответственность за предотвращение хищения, уничтожения или модификации биометрической информации. Указанные требования вступили в силу 7 января 2023 года — спустя три с половиной года после принятия базового закона.

Статья 27¹ Закона в редакции 2026 года закрепила требование об исключительно локальном хранении биометрических и генетических данных граждан Узбекистана: размещение такой информации на зарубежных серверах прямо запрещено. Для иных категорий персональных данных допускается трансграничное хранение при условии соблюдения установленных требований безопасности. Кроме того, в апреле 2025 года Указом Президента № РР-153 в финансовом секторе введены обязательные уведомления об утечках биометрических данных и установлена юридическая ответственность операторов за инциденты в сфере защиты информации.

Закон «О кибербезопасности» № ЗРУ-764 от 15 апреля 2022 года дополняет нормативную базу в части информационной безопасности при обработке чувствительных данных, к которым относятся и биометрические.

Надзорные функции в сфере персональных данных возложены на Агентство по персонализации при Министерстве внутренних дел Республики Узбекистан, которое ведёт Государственный реестр баз персональных данных и осуществляет контроль за соблюдением законодательства операторами. Вместе с тем правозащитные эксперты указывают на недостаточную независимость и ограниченные ресурсы надзорного органа, что снижает эффективность контроля на практике.

Наиболее фундаментальным пробелом узбекского права в рассматриваемой сфере является отсутствие самостоятельного нормативного акта, посвящённого исключительно биометрическим данным. Действующее регулирование осуществляется в рамках общего закона о персональных данных, нормы которого не учитывают специфику биометрической информации — её постоянства, невозможности замены, а также особых рисков, которые её несанкционированное использование создаёт для личности. Как справедливо отмечают исследователи, такая конструкция не создаёт достаточной нормативной базы для регулирования всего многообразия современных сценариев применения биометрических технологий.

Для сравнения: в Европейском союзе биометрические данные выделены в особую категорию в статье 9 Общего регламента о защите данных (GDPR), а Акт об искусственном интеллекте (AI Act) 2024 года вводит дополнительные ограничения на применение систем биометрической идентификации в общественных местах, классифицируя их как технологии высокого риска. Сравнительно-правовое исследование Темирова Р. (2024) убедительно показывает, что Узбекистан существенно отстаёт от стандартов ЕС в данном вопросе, находясь лишь на начальном этапе формирования специализированной нормативной базы.

Аналогичный вывод делают Гринлиф и Калдани (2025), указывая, что правовые режимы персональных данных всех шести центральноазиатских государств практически не получили критического научного анализа, а их нормативные решения нередко заимствуются из российского или китайского законодательства без необходимой адаптации.

На протяжении первых шести лет с момента принятия Закона «О персональных данных» его нормы в части биометрической информации носили в значительной мере декларативный характер. Реальный механизм принуждения к исполнению требований закона, соразмерная ответственность операторов биометрических систем за утечки и нарушения прав субъектов данных фактически отсутствовали. Ситуация начала меняться лишь в 2025 году: Указ Президента № РР-153 ввёл в финансовом секторе обязательные уведомления об инцидентах и юридическую ответственность за нарушения, ознаменовав, по оценке экспертов, «переход от декларативных норм к практической подотчётности».

Тем не менее данные требования распространяются пока лишь на финансовый сектор, оставляя другие отрасли — здравоохранение, транспорт, государственное управление — без аналогичных механизмов ответственности.

Существенной проблемой остаётся также размытость санкций за нарушения в сфере обработки биометрических данных. Административная ответственность, предусмотренная Кодексом об административной ответственности Республики Узбекистан, не дифференцирована с учётом особой опасности утечки именно биометрических данных по сравнению с иными категориями персональной информации. Между тем очевидно, что компрометация биометрического шаблона влечёт для субъекта значительно более тяжкие и необратимые последствия, нежели, например, утечка адреса электронной почты.

Законодательное требование о хранении биометрических данных граждан Узбекистана исключительно на территории страны появилось лишь в результате поправок 2026 года. До этого момента правовой режим трансграничной передачи биометрической информации определялся общими нормами статьи 27 Закона, которые допускали передачу персональных данных в иностранные государства, обеспечивающие «адекватную защиту» прав субъектов, без специальных ограничений для биометрики. Показательно, что норма о локализации биометрических данных была принята в том числе в контексте переговоров о допуске на узбекский рынок международных платёжных систем Apple Pay и Google Pay, — то есть её появление было обусловлено коммерческими, а не сугубо правозащитными мотивами. Данное обстоятельство свидетельствует о реактивном, а не проактивном характере законодательной политики в данной сфере.

Одним из наиболее острых пробелов действующего регулирования является полное отсутствие требований к прозрачности алгоритмов биометрической идентификации. Статья 24 Закона «О персональных данных» предоставляет субъекту право не подвергаться решениям, основанным исключительно на автоматизированной обработке его данных, — однако не устанавливает каких-либо требований к объяснимости таких решений, обязательному аудиту алгоритмов или независимой проверке точности биометрических систем. Между тем международный опыт убедительно свидетельствует о том, что системы распознавания лиц могут демонстрировать существенные погрешности в отношении отдельных групп населения, что создаёт реальный риск дискриминации и ошибочной идентификации. В отсутствие механизмов аудита и контроля точности такие риски остаются неуправляемыми.

Особую озабоченность вызывает применение биометрических систем в правоохранительной деятельности, где ошибочная идентификация может повлечь самые серьёзные правовые последствия для гражданина. Ни законодательство, ни ведомственные нормативные акты не регулируют порядок оспаривания результатов биометрической идентификации, не устанавливают стандартов допустимого уровня погрешности и не предусматривают обязательного участия человека в принятии решений на основании биометрических данных.

Базовым условием обработки биометрических данных в Узбекистане является согласие их субъекта. Вместе с тем действующее законодательство не устанавливает специальных требований к форме и содержанию такого согласия применительно к биометрической информации. Общая норма Закона допускает выражение согласия «в любой форме, позволяющей подтвердить факт его получения», — что существенно снижает стандарт защиты субъекта по сравнению, например, с требованиями GDPR о

«конкретном, информированном, недвусмысленном и добровольном» согласии, которое должно быть столь же легко отозвать, как и дать.

Критически важной остаётся и проблема реальной добровольности согласия. Во многих ситуациях — при получении государственных услуг, открытии банковского счёта или трудоустройстве — субъект данных фактически лишён возможности отказаться от предоставления биометрической информации без утраты доступа к соответствующему сервису. Такое «вынужденное согласие» по своей правовой природе не соответствует принципу свободного волеизъявления и не может считаться надлежащим правовым основанием для обработки чувствительных данных.

Самостоятельной проблемой является крайне слабая научная разработанность вопросов правового регулирования биометрических данных в Узбекистане и регионе в целом. Как указывают Гринлиф и Калдани (2025), правовые режимы персональных данных центральноазиатских государств практически не получили критического академического анализа, а существующие региональные исследования лишь вскользь упоминают их без детального сопоставления. Отсутствие развитой правовой доктрины в данной сфере затрудняет как разработку законодательных реформ, так и подготовку квалифицированных специалистов, способных применять и развивать соответствующее законодательство.

На основании проведённого анализа представляется возможным сформулировать следующие предложения по совершенствованию правового режима биометрических данных в Узбекистане.

Во-первых, необходимо принять специальный Закон Республики Узбекистан “О биометрических данных”, который бы учитывал уникальную правовую природу данной категории информации, устанавливал исчерпывающий перечень оснований для её обработки, конкретизировал форму и требования к согласию субъекта, а также закреплял специальные механизмы защиты прав граждан применительно к каждой сфере использования биометрических технологий — государственному управлению, финансам, здравоохранению, трудовым отношениям и правоохранительной деятельности.

Во-вторых, требуется создание независимого специализированного регулятора в сфере персональных и биометрических данных — по образцу органов защиты данных, действующих в государствах ЕС. Действующая модель, при которой надзорные функции возложены на Агентство по персонализации при МВД, порождает очевидный конфликт интересов: структура, являющаяся одним из крупнейших операторов биометрических данных в стране, одновременно осуществляет надзор за соблюдением законодательства в данной сфере.

В-третьих, необходимо законодательно закрепить требования к прозрачности и объяснимости алгоритмов биометрической идентификации, ввести обязательный независимый аудит таких систем, установить стандарты допустимого уровня погрешности и закрепить право субъекта на оспаривание результатов автоматизированной идентификации с обязательным участием человека в принятии окончательного решения.

В-четвёртых, санкции за нарушения в сфере обработки биометрических данных должны быть существенно дифференцированы с учётом особой тяжести возможных последствий для субъекта.

Целесообразно ввести повышенные штрафы за утечку биометрических данных, а также уголовную ответственность за их незаконный сбор, хранение или использование в корыстных целях.

В-пятых, требования о добровольности согласия должны быть конкретизированы применительно к ситуациям, в которых субъект фактически лишён возможности отказаться от предоставления биометрических данных. В таких случаях необходимо либо прямо запрещать обусловливание предоставления услуги согласием на биометрическую идентификацию, либо предусматривать обязательные альтернативные способы идентификации.

Биометрические данные представляют собой принципиально новый объект правового регулирования, требующий иного подхода по сравнению с традиционными персональными данными. Их уникальность, неизменяемость и прямая связь с физической личностью человека создают как беспрецедентные возможности для идентификации, так и беспрецедентные риски для прав и свобод граждан.

Правовой режим биометрических данных в Узбекистане за последние годы претерпел определённые позитивные изменения: приняты технические стандарты хранения, введены требования локализации, в финансовом секторе установлен механизм ответственности операторов. Однако эти шаги носят во многом реактивный и фрагментарный характер, не формируя целостной, системной и превентивной модели регулирования.

Разрыв между интенсивностью применения биометрических технологий и уровнем их правового регулирования создаёт реальную угрозу правам граждан. Устранение выявленных пробелов требует не точечных поправок в действующее законодательство, а комплексной реформы, результатом которой должна стать самостоятельная, специализированная и эффективно применяемая система правовой защиты биометрических данных — соответствующая как конституционным гарантиям права на неприкосновенность частной жизни, так и международным стандартам в данной сфере.

Реализация сформулированных предложений будет способствовать достижению целей стратегии «Цифровой Узбекистан — 2030», укреплению доверия граждан к цифровым сервисам и формированию правового государства, гарантирующего защиту фундаментальных прав личности в условиях цифровой экономики.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Закон Республики Узбекистан «О персональных данных» № ЗРУ-547 от 02.07.2019 г. (с изменениями и дополнениями 2021, 2023, 2026 гг.) // lex.uz. — URL: <https://lex.uz/docs/4396428>
2. Закон Республики Узбекистан «О кибербезопасности» № ЗРУ-764 от 15 апреля 2022 г. // lex.uz. — URL: <https://lex.uz/docs/5962966>
3. Указ Президента Республики Узбекистан № РР-153 от 30 апреля 2025 года «О дополнительных мерах по обеспечению кибербезопасности в финансовом секторе».

4. Постановление Кабинета Министров Республики Узбекистан № 2 от 2023 года «Об утверждении требований к материальным носителям биометрических и генетических данных и технологиям их хранения».
5. Конституция Республики Узбекистан (новая редакция, вступила в силу 1 мая 2023 г.).
6. Temirov R. Biometric Identification in Uzbekistan's Legal System // International Journal of Law and Policy. — 2024. — Vol. 2, No. 8. — DOI: 10.59022/ijlp.217
7. Greenleaf G., Kaldani T. Data privacy laws in Central Asia: between ex-SSR and 'Belt & Road' // International Data Privacy Law. — Oxford Academic. — 2025. — Vol. 15, Issue 1. — P. 67–90. — DOI: 10.1093/idpl/ipaf001
8. Правовые механизмы защиты персональных данных в Узбекистане // in-academy.uz. — URL: <https://in-academy.uz/index.php/cajar/article/download/53047/33678/58694> (дата обращения: 20.04.2026)
9. Биометрические данные в Узбекистане. Защита и безопасность // Legal Clinic UZ. — URL: <https://legalclinic.uz/tpost/tips570x41-biometricheskie-dannie-v-uzbekistane-zas> (дата обращения: 20.04.2026)
10. Локализация персональных данных в Узбекистане: переход к более гибкой модели регулирования // Settle Advisory. — 2026. — URL: <https://settleadvisory.com/ru/news-ru/lokalizatsiya-personalnykh-dannykh> (дата обращения: 20.04.2026)
11. Personal Data Compliance in Uzbekistan // The Legal 500. — 2025. — URL: <https://www.legal500.com/developments/thought-leadership/personal-data-compliance-in-uzbekistan/> (дата обращения: 20.04.2026)
12. Requirements for Protection of Personal Data in Uzbekistan // Azizov & Partners. — 2023. — URL: <https://azizovpartners.uz/en/memos/requirements-for-protection-of-personal-data-in-uzbekistan/> (дата обращения: 20.04.2026)
13. Data Protection Laws of the World: Uzbekistan // DLA Piper. — 2025. — URL: <https://www.dlapiperdataprotection.com/?t=law&c=UZ> (дата обращения: 20.04.2026)
14. Персональные данные в Республике Узбекистан // Workspace.ru. — 2024. — URL: <https://workspace.ru/blog/personalnye-dannye-v-respublike-uzbekistan/> (дата обращения: 20.04.2026)
15. Как смягчили закон о персональных данных в Узбекистане // Kursiv Media. — 2026. — URL: <https://uz.kursiv.media/2026-03-27/biometricheskie-i-geneticheskie-dannye-uzbekistanczev-zapretili-hranit-za-rubezhom/> (дата обращения: 20.04.2026)
16. Биометрия, блокировки и контроль сессий. Как в Узбекистане будут бороться с онлайн-мошенничеством // Gazeta.uz. — 2026. — URL: <https://www.gazeta.uz/ru/2026/01/21/anti-fraud/> (дата обращения: 20.04.2026)
17. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation — GDPR). — Official Journal of the European Union. — L 119. — 04.05.2016.