ОСОБЫЙ ПРАВОВОЙ РЕЖИМ ОБРАБОТКИ БИОМЕТРИЧЕСКИХ ДАННЫХ В УЗБЕКИСТАНЕ: СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ ОПЫТА ЕВРОПЕЙСКОГО СОЮЗА И КАЗАХСТАНА

Иброхимовой Назирахон
магистрант кафедры информационного права
Ташкентского государственного юридического университета.
naziraxon.ibroximova@gmail.com

https://doi.org/10.5281/zenodo.20561593

Аннотация. *Статья посвящена сравнительно-правовому анализу моделей регулирования биометрических данных в Европейском Союзе и Республике Казахстан с целью выработки рекомендаций для законодателя Узбекистана. Установлено, что европейская модель, основанная на GDPR и AI Act 2024 года, формирует про-активный трехуровневый режим защиты, тогда как казахская модель добросовестно воспроизводит европейские принципы при структурном пробеле – отсутствии специальных норм для биометрических систем. Узбекистан, располагая статусом «позднего регулятора», способен синтезировать достоинства обеих систем, избежав их недостатков. Сформулированы конкретные предложения de lege ferenda.*

Ключевые слова: *биометрические данные, правовой режим, GDPR, AI Act, Казахстан, Узбекистан, DPIA, Privacy by Design, сравнительное правоведение.*

Масштабное внедрение биометрических технологий в государственное управление, банковский сектор и системы безопасности превратило биометрические данные в один из главных правовых вызовов цифровой эпохи. Республика Узбекистан в рамках Стратегии «Цифровой Узбекистан – 2030» активно применяет биометрические системы: Единый государственный реестр населения, биометрические паспорта, системы распознавания лиц. Между тем Закон «О персональных данных» от 2 июля 2019 года № ЗРУ-547 лишь упоминает биометрические данные в статье 10 как особую категорию, не содержа ни операционального определения, ни специальных гарантий, ни механизмов контроля[1].

Цель статьи – на основе сравнительно-правового анализа опыта ЕС и Казахстана выявить типичные правовые проблемы и сформулировать конкретные рекомендации для законодателя Узбекистана. Применяемые методы: сравнительно-правовой, формально-юридический, анализ и синтез, системный подход. Теоретической основой служат труды Э.Дж. Кинд (KU Leuven), П. Шварца (UC Berkeley), И.Л. Бачило (ИГП РАН), А.Е. Кансейтова (КазНУ)[2].

Нормативную базу составляют: Регламент (ЕС) 2016/679 (GDPR); Регламент (ЕС) 2024/1689 об искусственном интеллекте (AI Act), вступивший в силу 1 августа 2024 года, запреты которого в части биометрии стали обязательными с 2 февраля 2025 года; Закон Республики Казахстан «О персональных данных и их защите» № 94-V от 21 мая 2013 года (ред. 2021); Закон «О персональных данных» Узбекистана 2019 года.

[1] Закон Республики Узбекистан «О персональных данных» от 2 июля 2019 года № ЗРУ-547, ст. 10; Указ Президента РУз «Об утверждении Стратегии «Цифровой Узбекистан – 2030»» от 5 октября 2020 года № УП-6079.

[2] Kindt E.J. Privacy and Data Protection Issues of Biometric Applications. – Dordrecht: Springer, 2013. P. 1–12; Бачило И.Л. Информационное право. 3-е изд. – М.: Юрайт, 2016. С. 214–220; Кансейтов А.Е. Правовое регулирование персональных данных в Республике Казахстан. – Алматы: Жеті жарғы, 2018. С. 3–10.

Для целей настоящего исследования «биометрические данные» понимаются в значении статьи 4(14) GDPR: персональные данные, полученные в результате специальной технической обработки, относящиеся к физическим, физиологическим или поведенческим характеристикам лица и позволяющие его уникальную идентификацию[3].

Доктринальную основу образуют: монография Э.Дж. Кинд, определившей биометрические данные через три кумулятивных признака (уникальные биологические характеристики автоматизированные средства + цели идентификации); работы Л. Бирлена по теории принципов защиты данных; труды казахских авторов А.Е. Кансейтова и Г.Т. Турсуновой о регулировании персональных данных в Центральной Азии[4].

Биометрические данные обладают четырьмя принципиальными правовыми свойствами: уникальностью (вероятность совпадения папиллярных узоров – 1 к 64 миллиардам), неизменяемостью (невозможно «сменить» при компрометации, в отличие от пароля), неотчуждаемостью от личности (ЕСПЧ в деле S. и Marper v. UK констатировал: даже хранение отпечатков затрагивает частную жизнь[5]) и способностью раскрывать чувствительную информацию – изображение лица неизбежно выдает расовое происхождение, голос – состояние здоровья. Именно эти свойства обусловливают необходимость особого, повышенного правового режима.

Европейская модель является мировым стандартом. Статья 9(1) GDPR запрещает обработку биометрических данных как правило, устанавливая исчерпывающие исключения – в том числе явное (explicit) согласие субъекта. Статья 35 обязывает к проведению DPIA (оценки воздействия на защиту данных) до начала обработки. Статья 25 закрепляет принцип Privacy by Design – интеграцию мер защиты на этапе проектирования системы. AI Act 2024 ввел прямой запрет дистанционной биометрической идентификации в общественных местах в режиме реального времени (статья 5(1)(d)); нарушение влечет штраф до 35 млн евро или 7 % глобального оборота[6].

Казахская модель добросовестно воспроизводит европейские принципы, однако содержит структурный пробел. Закон 2013 года определяет биометрические данные в статье 1 как «сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность» – без указания на автоматизированный характер обработки как квалифицирующий признак. Закон не предусматривает ни DPIA, ни принципа Privacy by Design, ни прямого запрета массовой идентификации. Надзорный орган лишен права самостоятельно налагать санкции: максимальный штраф – около 600 долл. США, что не создает реального превентивного воздействия на крупных операторов. Исследователь А.Е. Кансейтов характеризует это как «добросовестное воспроизведение принципов при недостаточном внимании к специфике биометрических систем»[7].

---

[3] Regulation (EU) 2016/679 (GDPR), Art. 4(14); Regulation (EU) 2024/1689 (AI Act), Art. 5 – prohibitions effective 2 February 2025; Закон РК «О персональных данных и их защите» № 94-V от 21 мая 2013 года (ред. 2021).

[4] Kindt E.J. Op. cit. P. 272–276; Bygrave L.A. Data Protection Law. – The Hague: Kluwer, 2002. P. 67–89; Турсунова Г.Т. Институциональные механизмы защиты персональных данных в Центральной Азии // Вестник КазНУ. – 2021. – № 4. – С. 67–79.

[5] ECtHR, S. and Marper v. United Kingdom, Grand Chamber, 4 December 2008, § 84.

[6] GDPR, Arts. 9(1), 9(2)(a), 25, 35; Regulation (EU) 2024/1689, Art. 5(1)(d), 99(3) – штраф до €35 млн / 7% оборота; запреты вступили в силу 2 февраля 2025.

[7] Закон РК «О персональных данных и их защите», ст. 1 п. 4; Кансейтов А.Е. Указ. соч. С. 155; Турсунова Г.Т. Указ. соч. С. 73–75.

Узбекистан воспроизводит проблемы казахской модели в более острой форме. Закон 2019 года не содержит легального определения биометрических данных, не обязывает к DPIA, не закрепляет принцип Privacy by Design, не предусматривает уведомления об инцидентах, не вводит ни запрета массовой идентификации, ни института DPO. Агентство по персональным данным также лишено права прямых санкций. Реформа локализации данных 2026 года, сохранившая абсолютное требование хранения на территории страны именно для биометрических данных, косвенно признает их особую чувствительность, однако специального процессуального регулирования не создала[8].

Сопоставление трех моделей обнаруживает общую закономерность: разрыв между декларируемым особым статусом биометрических данных и реальным уровнем их защиты. Европейская модель наиболее последовательно преодолевает этот разрыв, однако и она не лишена недостатков: сложность соблюдения требований для малых и средних операторов, регуляторная фрагментация между государствами-членами, высокие затраты на комплаенс. Digital Omnibus Европейской комиссии от 19 ноября 2025 года предложил скоординированные поправки к GDPR и AI Act с целью «упрощения без снижения стандартов защиты» – свидетельство того, что даже лидер признает необходимость баланса между охраной прав и операционной реализуемостью[9].

Казахская модель представляет для Узбекистана более близкий сравнительный пример: схожая правовая традиция, сопоставимый административный потенциал, общее постсоветское институциональное наследие. Именно казахский опыт наглядно показывает: воспроизведение европейских принципов без специальных процессуальных норм для биометрических систем создает лишь иллюзию защиты. Профессор Бачило точно заметил: «Необратимость ущерба от раскрытия информации является ключевым критерием установления повышенного режима ее охраны» – применительно к биометрическим данным это наблюдение носит абсолютный характер[10].

Статус «позднего регулятора» предоставляет Узбекистану уникальную возможность: строить систему с учетом чужих ошибок, а не вопреки им. Профессор П. Шварц указывает: «Государства, формирующие законодательство о данных во второй волне цифровизации, имеют исключительную возможность построить более сбалансированные системы». Это возможно, однако требует сознательного законодательного выбора: не «переписывания» GDPR или казахского закона, а функционального заимствования – адаптации проверенных инструментов к реальному административному потенциалу[11].

На основании проведенного анализа формулируются следующие выводы и рекомендации de lege ferenda для Республики Узбекистан.

Во-первых, необходимо ввести в статью 3 Закона «О персональных данных» трехэлементное определение биометрических данных по образцу GDPR: специализированная техническая обработка + биологические, физиологические или поведенческие характеристики + уникальная идентификация личности.

[8] Закон РУз «О персональных данных» № ЗРУ-547, ст. 10; ПКМ РУз № 570 от 5 октября 2022 года; поправки о локализации данных, 2026 год.
[9] European Commission. Digital Omnibus Package. Brussels, 19 November 2025; Biometric Update, 'EU pushes AI Act deadlines for high-risk systems', May 2026.
[10] Бачило И.Л. Указ. соч. С. 215.
[11] Schwartz P.M. Global Data Privacy: The EU Way // New York University Law Review. – 2019. – Vol. 94. – P. 810.

Открытый характер определения («и иные аналогичные данные») обеспечит технологическую нейтральность и охватит новые виды биометрии без изменения закона[12].

Во-вторых, следует ввести обязательную оценку воздействия на защиту данных (DPIA) до начала обработки биометрических данных – для всех государственных систем и для частных операторов, обрабатывающих биометрию более 5 000 субъектов в год.

Именно отсутствие DPIA является принципиальным отличием казахской модели от европейской и главным структурным пробелом узбекского законодательства[13].

В-третьих, необходимо закрепить запрет дистанционной биометрической идентификации в общественных местах в режиме реального времени по образцу статьи 5(1)(d) AI Act, допустив исключения исключительно на основании судебного решения и в строго ограниченных случаях.

Данная норма является важнейшей гарантией против превращения биометрии в инструмент тотального наблюдения.

В-четвертых, требует усиления институциональный механизм: Агентство по персональным данным должно быть наделено правом самостоятельного наложения санкций, а для операторов, осуществляющих масштабную биометрическую обработку, следует ввести обязательный институт Сотрудника по защите данных (DPO).

Реализацию предложенных мер целесообразно осуществлять поэтапно: в 2025–2026 годах – определение и стандарт явного согласия; в 2026–2028 годах – DPIA и запрет массовой идентификации; в 2028–2030 годах – технический регламент и присоединение к Конвенции Совета Европы № 108[14].

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Закон Республики Узбекистан «О персональных данных» от 2 июля 2019 года № ЗРУ-547.
2. Конституция Республики Узбекистан (в ред. 2023 года), ст. 27, 30.
3. Regulation (EU) 2016/679 (GDPR). OJ L 119, 4.5.2016.
4. Regulation (EU) 2024/1689 (Artificial Intelligence Act). OJ L, 12.7.2024.
5. Закон Республики Казахстан «О персональных данных и их защите» № 94-V от 21 мая 2013 года (в ред. 2021 года).
6. European Commission. Digital Omnibus Package. Brussels, 19 November 2025.
7. ECtHR, S. and Marper v. United Kingdom, Grand Chamber, 4 December 2008.
8. Kindt E.J. Privacy and Data Protection Issues of Biometric Applications. – Dordrecht: Springer, 2013.
9. Bygrave L.A. Data Protection Law. – The Hague: Kluwer Law International, 2002.
10. Schwartz P.M. Global Data Privacy: The EU Way // NYU Law Review. – 2019. – Vol. 94. – P. 771–818.
11. Бачило И.Л. Информационное право. 3-е изд. – М.: Юрайт, 2016.
12. Кансейтов А.Е. Правовое регулирование персональных данных в РК. – Алматы: Жеті жарғы, 2018.

[12] GDPR, Art. 4(14); Kindt E.J. Op. cit. P. 272–276

[13] GDPR, Art. 35(3)(b); Article 29 Data Protection Working Party, WP 248 rev.01, Guidelines on DPIA, 4 October 2017. P. 11.

[14] GDPR, Arts. 37(1)(c), 83; Regulation (EU) 2024/1689, Art. 5(1)(d); Convention No. 108+ (CETS No. 223), Council of Europe, 2018.

13. Турсунова Г.Т. Институциональные механизмы защиты персональных данных в Центральной Азии // Вестник КазНУ. – 2021. – № 4.
14. WP 29, Guidelines on DPIA, WP 248 rev.01, 4 October 2017.