DOI: 10.51634/2307-5201_2025_4_31
УДК 341.231.14
МРНТИ 81.93.29

ЗАЩИТА БИОМЕТРИЧЕСКИХ ДАННЫХ: АНАЛИЗ ЗАКОНОДАТЕЛЬСТВА КАЗАХСТАНА В КОНТЕКСТЕ ЗАРУБЕЖНОЙ ПРАКТИКИ

Д. УТЕГЕН, PhD докторант, Teaching Professor Высшей школы права Maqsut Narikbayev University (Республика Казахстан, г. Астана), e-mail: d_utegen@kazguu.kz

Актуальность исследования обусловлена повсеместным и активным внедрением биометрических технологий в различных сферах для идентификации личности и отсутствием комплексного правового регулирования в Республике Казахстан.

Предметом анализа выступает законодательство Казахстана в области обработки, хранения и использования биометрических данных, а также международная практика в данной сфере.

Целью статьи является выявление правовых рисков, связанных с применением систем биометрической аутентификации, и формулирование предложений по их правовому регулированию. В качестве методов исследования применялись сравнительно-правовой анализ, кейс-стади и нормативно-догматический подход.

В статье проанализирован опыт регулирования биометрических данных в Европейском союзе, Российской Федерации и отдельных штатах США, уделяющих внимание защите биометрических данных. Особое внимание посвящено судебной практике, связанной с неправомерным использованием биометрической информации частными и государственными структурами.

Научная новизна работы заключается в том, что в результате проведённого анализа сформулированы выводы о необходимости совершенствования национального законодательства и внедрения механизмов надзора за биометрическими системами.

Ключевые слова: идентификация, биометрическая аутентификация, биометрические данные, приватность, персональные данные, неприкосновенность частной жизни.

Введение

Увеличение объёма цифровых операций и электронных платежей повлияло на внедрение различных систем цифровой идентификации. Автоматизированная проверка и идентификация личности производится при использовании различных приложений. Доступ к оплате общественного транспорта, получение государственных услуг, предоставление персональной информации при прохождении границ, в аэропорту, при использовании веб-приложений, при онлайн-банкинге, онлайн-покупках и других операциях осуществляется процесс биометрической аутентификации.

В мире повсеместно внедряется технология распознавания лица, идентификация при помощи отпечатков и сетчатки глаз. Также наряду с традиционными методами идентификации, применяются способы верификации через биологические характеристики человека на основе физических, биологических или поведенческих особенностей человека. Биометрические данные наиболее распространенно применяются правоохранительными органами в целях обеспечения национальной безопасности, расследования преступлений, для охраны общественного порядка, предотвращения совершения правонарушений [1].

Биометрические признаки включают отпечатки пальцев, лицо, голос, радужную оболочку глаза и другие биологические признаки. Преимуществом использования биометрических данных для проверки личности является то, что они просты в использовании, так как пользователям не нужно запоминать или записывать пароли, пин-коды или иметь при себе свои идентификационные карты [2, 3].

© Д. Утеген, 2025

Отпечаток пальца является биометрическим идентификатором, определяемым как «уникальная физическая характеристика человека, которая используется для идентификации личности» [4,5]. Отпечатки пальцев являются наиболее распространенными среди биометрических идентификаторов, тем не менее идентификация также включает сканирование сетчатки глаз, голос, лицо, узоры ладоней и рисунок вен.

После пандемии COVID-19 использование биометрических данных увеличилось, технологию применяли как средство поддержания социальной дистанции при карантинных мерах [6]. В 2018 г. 62% компаний использовали различные формы технологий биометрической аутентификации [7]. Преимуществом системы стала удаленная идентификация как в сфере получения государственных услуг, так в финансовой и социальной среде.

В Казахстане последствия пандемии COVID-19 способствовали созданию цифровых решений по удаленной идентификации личности. При Национальном Банке Республики Казахстан был создан «Центр обмена идентификационными данными» [8]. Внедрен сервис Digital ID Министерства цифрового развития и аэрокосмической промышленности РК. Сервис центра обмена идентификационными данными (ЦОИД) позволяет банкам второго уровня проводить удаленную идентификацию личности клиентов, открывать банковские счета и вклады, осуществлять кредитование, выпуск платежных карточек и другие операции [9].

Основные положения

Материалы и методы исследования

В данной статье проведен анализ законодательной базы Республики Казахстан в контексте регулирования процессов обработки биометрических баз данных граждан. В ходе анализа выработаны рекомендации по контролю за безопасностью данных и выявлению угроз, связанных с возможной утечкой биометрических баз данных.

В контексте сравнения зарубежного опыта по правовым подходам к регулированию биометрических баз данных и судебным разбирательствам, направленным на предотвращение нарушений прав человека, были применены методы эмпирического анализа, включающие в себя анализ статистических данных и отчетов о случаях утечек персональных данных [10].

Также проведен нормативно-правовой анализ законодательной базы Республики Казахстан. Для получения более широкого контекста проведено международное сравнение с опытом стран, которые уже имеют опыт применения систем идентификации. Анализ судебных разбирательств с учетом юридических последствий связанных с нарушениями в области биометрических данных.

Основные методы включают риск-ориентированный подход, сравнительно-правовой анализ и юридическое прогнозирование. Риск-ориентированный подход позволяет выявить и оценить потенциальные риски, связанные с использованием биометрических данных, и прогнозировать угрозы, возникающие в результате дальнейшего распространения технологий биометрической аутентификации.

Сравнительно-правовой анализ используется для сопоставления правовых моделей и подходов, применяемых в различных странах и объединениях, таких как Европейский Союз, Соединенные Штаты Америки и Российская Федерация. Этот метод позволяет выявить лучшие практики и методы правового регулирования, которые могут быть адаптированы для применения в Республике Казахстан.

Обсуждение

Российская Федерация:

В России с 30 декабря 2021 г. действует Единая биометрическая система (ЕБС – далее) используемая для предоставления государственных и муниципальных услуг [11]. С 1998 г. в Российской Федерации действует закон о государственной дактилоскопической регистрации, также отдельно был принят закон о государственной геномной регистрации. С аналогичной системой можно сравнить центр Fusion, применяемый в США. Центры Fusion используют инструменты интеллектуального анализа данных для процессов обработки персональных данных из государственных и частных баз, Интернета, и открытых источников». Центр Fusion также имеет доступ к масштаб-

ному количеству данных субъектов. Там же осуществляется сбор биометрических данных в целях применения программного обеспечения для распознавания лиц [12].

Одним из важных рисков наличия баз данных и сервисов в государстве является отсутствие должной защиты биометрических данных, в результате которых может быть нарушено право на неприкосновенность частной жизни как граждан, так и иностранных граждан. Также в России более трех миллионов граждан согласились предоставить согласие на обработку персональных биометрических данных, однако одним из ключевых правовых рисков, связанных с функционированием Единой биометрической системы (ЕБС) в России является централизация чувствительных персональных данных в рамках одной государственной платформы [13]. Как отмечают Петрова и Юртаев, такая архитектура порождает значительные уязвимости, риски утечек и несанкционированного доступа и потенциального злоупотребления полномочиями со стороны государственных органов. Несмотря на заявленные цели по упрощению идентификации и расширению цифровых услуг со стороны государства, концентрация контроля над биометрическими данными усиливает опасения по поводу массового наблюдения и недостаточной прозрачности процессов обработки биометрическими данными. Кроме того, отсутствие чётких процедур получения согласия и принципов минимизации данных ставит под сомнение соответствие ЕБС как национальным конституционным нормам, так и международным стандартам в области права на неприкосновенность частной жизни [14].

Практика реализации ЕБС в России наглядно демонстрирует отсутствие единых стандартов и механизмов контроля. Ситуация приводит к ограниченной транспарентности, централизованному управлению данными и росту общественного недоверия. В этом контексте выработка и внедрение национальных стандартов в сфере защиты персональных и биометрических данных становится неотъемлемым условием для формирования правовой среды, обеспечивающей как развитие цифровых сервисов, так и соблюдение фундаментальных прав личности.

На основании анализа характерных особенностей и тенденций в России следует вывод о необходимости создания в России национальных стандартов в области защиты данных [15]. Данный подход позволит создать более четкий механизм взаимодействия участников обмена данными как в государственном, так и в частном секторе. Данная стратегическая цель будет стимулировать к наиболее эффективному использованию баз данных, способствовать расширению благоприятной среды для обмена данными между представителями частного сектора и государственными органами в пределах соблюдения требований и принципов обработки данных. А также соблюдать применение мер недискриминационного характера к персональным данным, основанной на политике недопущения дискриминации, безграничного доступа и согласованности в части правовых и технических аспектов регулирования трансграничного обмена данными.

Соединенные Штаты Америки:

Что касается практики США, то она носит разный характер, как и подходы по регулированию приватности, учитывая отсутствие федерального регулирования биометрических данных. Несмотря на многочисленные виды использования биометрических данных в Соединенных Штатах только некоторые штаты успешно применяют законы о защите биометрических данных [16, 17].

Закон о конфиденциальности биометрической информации штата Иллинойс (BIPA), известный как BIPA, обеспечивает кроме общей защиты биометрических данных возможность подавать частным лицам иски о возмещении ущерба за нарушение законодательства по биометрическим данным [18]. Законодательство, регулирующее получение и использование биометрии Capture or Use of Biometric Identifier Act (CUBI) [19], также имеет схожесть с BIPA. Вместо этого CUBI предписывает штраф в размере не более 25 000 долларов США за каждое нарушение [20].

Принятый Калифорнийский закон о конфиденциальности потребителей (CCPA) от 2018 года обеспечивает защитные меры для персональных данных потребителей, включая биометрические данные. В закон было внесено много поправок для уточнения его технических аспектов, тем не менее он достаточно обеспечивает средства защиты, аналогичные Общему регламенту Европейского союза по защите данных (GDPR) [21].

Анализ судебной практики США в сфере защиты биометрических данных позволяет выделить показательное дело, рассмотренное в федеральном суде штата Иллинойс, в рамках которого был предъявлен коллективный иск против двух американских компаний, использовавших биометрические технологии без соблюдения требований закона. Речь идет о нарушении положений Закона штата Иллинойс о защите биометрической информации (Biometric Information Privacy Act – BIPA), одного из самых строгих нормативных актов в этой сфере. Суть дела заключалась в том, что в ряде торговых автоматов, установленных на территории штата, использовались сканеры отпечатков пальцев для аутентификации покупателей при покупке товаров. При этом компании не обеспечили получение информированного письменного согласия пользователей на сбор и хранение их биометрических данных, как это предусмотрено BIPA. Кроме того, не были предоставлены данные о сроках хранения и порядке уничтожения такой информации.

В результате разбирательства суд признал действия компаний нарушающими BIPA, поскольку каждое отдельное сканирование отпечатка без согласия рассматривалось как отдельное нарушение закона.

По итогам дела было постановлено взыскать с ответчиков суммарный штраф в размере 6,8 миллиона долларов США, который распределялся между участниками коллективного иска. Это дело не только продемонстрировало реальную возможность привлечения к ответственности за нарушение биометрического законодательства, но и подтвердило высокую правовую значимость получения согласия и соблюдения принципов обработки персональных данных, особенно когда речь идет о биометрической идентификации в повседневной коммерческой деятельности [23].

В одном из наиболее известных дел в Иллинойсе против компании Facebook (ныне Meta) был предъявлен иск на сумму 650 миллионов долларов. Основанием послужило использование технологии распознавания лиц и автоматического проставления тегов изображений без уведомления пользователей. А был представлен иск в части сбора и хранения биометрических данных без получения согласия субъектов. Подобные примеры из международной практики демонстрируют высокий уровень ответственности за нарушение прав в сфере обработки особо чувствительных данных. В отличие от этого в Казахстане размер штрафных санкций в случае подобных разбирательств существенно ниже, что делает их сравнительно незначительными для крупных высокотехнологичных компаний [24].

Законодательство о защите биометрических данных в США сталкивается с несколькими основными проблемами. С одной стороны, законодательство слишком медленно борется со скоростью, с которой они собираются и обрабатываются [25]. С другой стороны, их различные виды могут быть защищены в определенных случаях, но наносить вред пользователям в связи с отсутствующим отдельным законом о защите биометрических данных [26]. К примеру, если некоторые государства будут принимать отдельные законы о защите биометрических данных, как в Европейском Союзе или на примере штатов Калифорния, Иллинойс и Техаса, а другие государства допустим нет. То произойдет то, что некоторые государства будут внедрять более строгие стандарты, чем другие. В результате государства, которые медленнее принимают законы, будут уязвимы от незащищенной обработки биометрических данных.

Европейский Союз:

Общий регламент по защите персональных данных GDPR направлен на защиту прав граждан ЕС от нарушений конфиденциальности данных. Основные изменения GDPR включают: расширение территориального охвата (экстерриториальная применимость), штрафы, согласие, уведомление о нарушении, право на доступ, право на забвение, переносимость данных, политики конфиденциальности и требование к компаниям назначать сотрудника по защите данных [27].

Сфера действия GDPR распространяется не только на компании, расположенные в Европейском союзе, которые обрабатывают персональные данные субъектов, проживающих в ЕС, но и на компании, расположенные за пределами ЕС, при условии, что они обрабатывают данные субъектов ЕС. GDPR также требует, чтобы предприятия, не расположенные в пределах Европейского Союза, но которые обрабатывают данные граждан ЕС, назначали представителя или открыли представительство в ЕС [28].

GDPR налагает штрафы на организации, которые не соблюдают требования в размере до четырех процентов от их годового оборота или двадцати миллионов евро. В GDPR используется многоуровневый подход к штрафам, штрафы применяются к контроллерам и процессорам. Кроме того, согласие возможно будет так же легко отозвать, как и дать его [29].

Что касается прав субъектов данных, GDPR предоставляет право на уведомление о нарушении права на доступ, право на забвение и право на переносимость данных [30]. Эти права требуют, что все государства-члены должны будут уведомлять субъектов и контролеров об утечках данных или инцидентах уязвимости в течении семидесяти двух часов [31,32]. Субъекты данных также имеют право на бесплатную копию хранения своих персональных данных в электронном формате [33]. Если субъекты данных соответствуют условиям, они имеют право на то, чтобы контроллер данных удалил данные субъекта, и прекратил дальнейшее распространение и прекращение обработки указанных данных [34,35].

Тем самым мы видим всеобъемлющий подход к процессам защиты персональных данных в ЕС, который позволяет контролировать и предотвращать риски, связанные с действиями наущающими право на конфиденциальность и защиту данных.

Анализ существующей ситуации в Казахстане:

В настоящее время не существует отдельных законов, защищающих биометрические данные субъектов в Казахстане [36]. Несмотря на то, что Закон о защите персональных данных охватывает регулирование сферы персональных данных в Казахстане и защищает персональную информацию государственных субъектов. Тем не менее в частном секторе такой защиты нет, как в нашем государстве, так и в практике зарубежных государств [37].

По части защиты персональных данных предусмотрена уголовная и административная ответственность, а также уголовная ответственность за правонарушения, связанные с посягательством на неприкосновенность частной жизни [38, 39].

Кроме наличия не совсем проработанных законодательных мер отмечается низкий уровень правоприменительной практики по защите приватности и персональных данных, а также отмечается невысокий уровень правового сознания и осведомленности граждан [40]. В рамках проведенных опросов среди граждан в Казахстане продемонстрирован низкий уровень осведомленности граждан о защите персональных данных 47% респондентов имеет представление о персональных данных и их защите, а 33% из них продемонстрировали низкие знания механизмов по защите права на приватность. Также 68% респондентов показали отсутствие знаний по кибергигиене, тем самым демонстрируя слабые знания действующих механизмов предотвращения правонарушений со стороны злоумышленников и третьих лиц. Также в вопросе осведомленности об утечке данных в сеть около 48% рецензентов отметили, что не были осведомлены о подобных случаях или в целом выражали безразличность к подобным случаям [41].

Важно отметить, что в Казахстане уже осуществляется сбор биометрических данных на добровольной основе. Сбор производится путем дактилоскопической регистрации всех граждан, проживающих на территории страны, а также иностранцев и лиц без гражданства. Согласно Закону о дактилоскопической и геномной регистрации дактилоскопическая регистрация граждан состоялась с 2024 года путем организации работы специализированной базы данных на добровольной основе [42, 43].

Результаты

Переходя к прикладному характеру представленных исследований, следует отметить, что указанный анализ также проведен в рамках информационной кампании «Биометрия KZ», участницей которого является автор статьи. В ходе информационной кампании было осуществлены брифинги, интервью и исследования по разъяснению норм положений профильного законодательства с определением более доступного понятийного аппарата для гражданского общества, связанного с дактилоскопической и геномной регистрацией данных [44]. В ходе проекта основной акцент поставлен на разъяснительной практике и расширении осведомленности аудитории путем публикации дополнительного информационно-образовательного контента.

В ходе информационной кампании было подготовлено исследование «возможных экономических, социальных и правовых последствий закона РК о дактилоскопической и геномной регистрации» [45]. Кроме общего аналитического исследования был проведен анализ законодательства Республики Казахстан на порядок соответствия международным стандартам в области защиты персональных данных. Комплексное исследование заключается в иллюстрации основных проблем и оценки рисков, связанных с созданием «АИС БИЛ». Приведены примеры из судебной практики, сформулированы общие рекомендации по соблюдению правил и применения этих положений для лиц, занимающихся сбором персональных данных.

В случае дальнейшей реализации вступившего в силу закона о дактилоскопической регистрации информационная кампания должна послужить катализатором к защите от несанкционированного контроля и слежки за гражданами, и устранить риски, связанные с неосведомленностью граждан о возможных угрозах приватности и защите персональных данных.

Заключение

Обсуждение имеющегося опыта зарубежных государств по защите персональных данных указывает на действующий разрозненный фрагментарный подход к защите персональных данных, который может негативно отразиться на порядке использования уникальной идентифицирующей биометрической информации. В сложившейся судебной национальной практике отмечается низкий уровень обращений для защиты биометрических данных. В сравнении с другими государствами можно увидеть определенные сложности судебных разбирательств против частных компаний. Если представить случай подачи иска от граждан Казахстана против частных компаний, допустим Meta, как была описана ранее подача иска от жителей штата Техас в США, то следует учесть значительно высокий уровень штрафов за нарушения политики приватности. И конечно же следует понимать, что штрафы, предусмотренные в рамках отраслевого законодательства, носят очень низкий уровень ответственности за правонарушения в области защиты данных в Казахстане. В качестве выводов данной статьи можно сформулировать следующие рекомендации:

– необходимо разработать общепринятые стандарты соблюдения требований контроля защиты биометрических данных в рамках разрабатываемого проекта закона по искусственному интеллекту;

– уполномоченным органом в сфере приватности обеспечить внеплановые и плановые проверки и мониторинг в отношении операторов, осуществляющих процесс обработки и хранения биометрических данных;

– предупреждать факты избыточного сбора данных, ограничить сбор биометрических данных без явно выраженного согласия субъекта;

– увеличить объем административных штрафов за нарушение сбора, передачи и иных процессов обработки данных,

– усилить контроль за несанкционированным получением информации третьими лицами и незаконной передачи биометрических данных субъекта.

– обратить внимание на порядок хранения данных на территории РК, обеспечить их сохранность и ограничить доступ для третьих лиц и порядок локализации.

Д. Утеген, Maqsut Narikbayev University Құқық жоғары мектебінің Teaching Professor (Астана қ., Қазақстан Республикасы): **Биометриялық деректерді қорғау: Қазақстан заңнамасын шетелдік тәжірибе контекстінде талдау.**

Зерттеудің өзектілігі биометриялық технологиялардың жеке тұлғаны сәйкестендіру саласына белсенді енгізілуімен және Қазақстан Республикасында бұл бағыттағы кешенді құқықтық реттеудің болмауымен негізделеді.

Зерттеудің нысаны ретінде Қазақстанның биометриялық деректерді өңдеу, сақтау және пайдалану саласындағы заңнамасы, сондай-ақ осы саладағы халықаралық тәжірибе қарастырылады.

Мақаладағы зерттеудің мақсаты — биометриялық аутентификация жүйелерін қолдануға байланысты құқықтық тәуекелдерді анықтап, оларды құқықтық реттеу бойынша ұсыныстар әзірлеу. Зерттеу барысында салыстырмалы-құқықтық талдау, кейс-стади және нормативтік-догматикалық әдістер қолданылды.

Мақалада Еуропалық одақтағы (GDPR үлгісінде), Ресей Федерациясындағы және АҚШ-тың жекелеген штаттарындағы биометриялық деректерді реттеу тәжірибесі талданған. Мемлекеттік және жекеменшік құрылымдар тарапынан биометриялық ақпаратты заңсыз пайдалану бойынша сот тәжірибесіне ерекше назар аударылды.

Зерттеудің ғылыми жаңашылдығы — биометриялық жүйелерге тәуелсіз бақылау тетіктерін енгізу және ұлттық заңнаманы жетілдіру қажеттілігі туралы қорытындыларды ұсынуда.

Түйін сөздер: идентификация, биометриялық аутентификация, биометриялық деректер, құпиялылық, дербес деректер, жеке өмірге қол сұқпау.

D. Utegen, PhD candidate, Teaching Professor, Higher School of Law, Maqsut Narikbayev University (Astana, Republic of Kazakhstan): Biometric data protection: a legal analysis of Kazakhstan in light of comparative international practice.

the relevance of this research lies in the rapid implementation of biometric technologies in the field of personal identification and the absence of comprehensive legal regulation in the Republic of Kazakhstan.

This article analyzes Kazakhstan's legislation governing the processing, storage, and use of biometric data, alongside international practices in this area.

The objective of the study is to identify legal risks associated with the use of biometric authentication systems and to propose legal solutions to mitigate these risks. The methodology includes comparative legal analysis, case studies, and a normative doctrinal approach.

The paper examines the regulatory frameworks for biometric data in the European Union (using the GDPR as an example), the Russian Federation, and selected U.S. states. Particular attention is paid to judicial practice involving the unlawful use of biometric information by public and private entities.

The novelty of this study lies in its findings regarding the necessity to improve national legislation and to introduce oversight mechanisms for biometric systems.

Keywords: identification, biometric authentication, biometric data, privacy, personal data, right to private life.

Список литературы:

1. Галиуллина Д.Р. Биометрические персональные данные. Документ. Архив. История. Современность. 2015. № 15. С. 264–268. URL:https://elar.urfu.ru/bitstream/10995/32968/1/dais-2015-15-22.pdf (07.06.2025).

2. Inc, Spiceworks. "Data Snapshot: Biometrics in the Workplace Commonplace, but Are They Secure?" The Spiceworks Community. URL: https://community.spiceworks.com/security/articles/2952-data-snapshot-biometrics-in-the-workplace-commonplace-but-are-they-secure/ (27.03.2025).

3. "Биометрические персональные данные и технологии идентификации: какие правовые проблемы могут возникнуть?"

4. Хелен Д. Борьба с терроризмом, санкции и война. International Review. 2021. № 916–917. С. 805–846, URL: https://international-review.icrc.org/sites/default/files/reviews-pdf/2023-06/IRRC_916-917_RU_805-846_Katja_Lindskov_Jacobsen.pdf (27.03.2025).

5. Burt, Chris. "Global Biometrics Market Forecast to Surpass \$82 B by 2027 despite Pandemic | Biometric Update."14 Oct. 2020. URL: https://www.biometricupdate.com/202010/global-biometrics-market-forecast-to-surpass82b-by-2027-despite-pandemic (27.03.2025).

6. Салихов Д.Р. Пандемия и персональные данные: как распространение новой коронавирусной инфекции бросает новые вызовы персональным данным // Конституционное и муниципальное право. 2021. № 3. – С. 46–50. URL: https://publications.hse.ru/articles/459709669 (09.06.2025).

7. "Biometric Data and COVID-19 in the Workplace." JD Supra. URL: https://www.jdsupra.com/legalnews/biometric-data-and-covid-19-in-the-86112/ (17.03.2025).

8. "Нацбанк: В пилотном режиме запущен сервис центра обмена идентификационными данными." Деловой портал Капитал.кз. URL: https://kapital.kz/tehnology/86517/natsbank-v-pilotnom-rezhime-zapushchen-servis-tsentra-obmena-identifikatsionnymi-dannymi.html (14.05.2025).

9. Постановление Правительства Республики Казахстан от 12 декабря 2017 г. № 827 «Об утверждении Государственной программы "Цифровой Казахстан"» (с изменениями и дополнениями по состоянию на 01.10.2020 г.) URL: https://online.zakon.kz/Document/?doc_id=37168057 (14.03.2025).

10. Сборник практических рекомендаций Организации Объединенных Наций по ответственному использованию биометрических данных и обмену ими в рамках борьбы с терроризмом. URL: https://www.unodc.org/pdf/terrorism/Compendium-Biometrics/_.pdf (26.04.2025).

11. 'В России заработала единая государственная система биометрии' (Ведомости, 30 Dec. 2021) URL: https://www.vedomosti.ru/society/news/2021/12/30/903427-putin-podpisal-zakon-o-biometrii (07.08.2025).

12. Department of Homeland Security. "Fusion Centers." Department of Homeland Security, 19 Sept. 2019. URL: https://www.dhs.gov/fusion-centers (23.05.2025).

13. Мифы и опасения: почему россияне боятся биометрии. Legalacademy.ru. URL: https://legalacademy.ru/sphere/post/mify-i-opaseniya-pochemu-rossiyane-boyatsya-biometrii (31.07.2025).

14. Петрова Д.А., Юртаев В.А. Unified Biometric System: Legal Regulation and Functions Problems. European Proceedings of Social and Behavioural Sciences. 2022. Vol. 139. – С. 712–719. DOI: 10.15405/epsbs.2022.06.84 URL: [https://doi.org/10.15405/epsbs.2022.06.84] (https://doi.org/10.15405/epsbs.2022.06.84).

15. Шилина С. Углубляясь в прошлое, размышляя о настоящем и исследуя культурные нюансы: Многогранное исследование биометрической проверки личности. Исследовательский институт «Парадигма». 2024. – 58 с. URL: https://www.researchgate.net/publication/377974352_Delving_into_the_past_pondering_the_present_and_probing_cultural_nuances_The_multi-faceted_exploration_of_biometric_identity_verification (09.06.2025).

16. Considerations for Fusion Center and Emergency Operations Center Coordination Comprehensive Preparedness Guide (CPG) 502. URL: https://www.fema.gov/media-library/assets/documents/25907 (01.06.2025).

17. U.S. Department of Justice. "Privacy Act of 1974." Justice.gov, 17 July 2015. URL: https://www.justice.gov/opcl/privacy-act-1974 (02.06.2025).

18. "Biometric Information Privacy Act (BIPA)." ACLU of Illinois, 26 Apr. 2021. URL: https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa (30.03.2025).

19. The Capture or Use of Biometric Identifiers Act (CUBI). 15 Sept. 2021. URL: https://www.caseguard.com/articles/the-capture-or-use-of-biometric-identifiers-act-cubi (13.05.2025).

20. Применение закона Техаса о биометрии сосредоточено на искусственном интеллекте. Holland & Knight LLP, 10 ноября 2022 г. URL: https://www.hklaw.com/en/insights/publications/2022/11/texas-enforcement-of-biometric-law-focuses-on-artificial-intelligence (31.07.2025).

21. "California Consumer Privacy Act (CCPA)." Google Cloud. URL: https://cloud.google.com/security/compliance/ccpa (22.05.2025).

22. "Власти США ополчились на Facebook за нелегальное распознавание лиц пользователей." CNews.ru. URL: https://www.cnews.ru/news/top/2022-02-25_vlasti_ssha_opolchilis_na (17.05.2025).

23. Неджафзаде Н., Кашиани Х. Face Image Quality Vector Assessment for Biometrics Applications. 2023 IEEE/CVF Winter Conference on Applications of Computer Vision Workshops (WACVW), США. 2023. – С. 511–520. DOI: 10.1109/WACVW58289.2023.00057 URL: https://doi.org/10.1109/WACVW58289.2023.00057 (17.05.2025).

24. "В США подан иск к Amazon, Google и Microsoft из-за сбора конфиденциальных сведений." РАПСИ. URL: https://rapsinews.ru/international_news/20200715/306034494.html (18.05.2025).

25. Biometrics Litigation: An Evolving Landscape | Practical Law \ URL: https://content.next.westlaw.com/practical-law/document/Id18ae0a6f51711e598dc8b09b4f043e0/Biometrics-Litigation-An-Evolving-Landscape?viewType=FullText\&transitionType=Default\&contextData=(sc.Default) (14.07.2025).

26. Грей Д., Ситрон Д. Разбитое зеркало: Подводные камни и потенциал мозаичной теории приватности в рамках Четвёртой поправки. North Carolina Journal of Law & Technology. 2013. Т. 14, № 2. – С. 381. URL: https://scholarship.law.unc.edu/ncjolt/vol14/iss2/3/ (23.06.2025).

27. Детерманн Л. Руководство по законодательству о защите данных: Международное корпоративное соответствие. 5-е изд. 2018. – 340 с.

28. Кузнецова С.С., Мочалов А.Н., Саликов М.С. Биометрическая идентификация в интернете: тенденции правового регулирования в России и за рубежом // Вестник Томского государственного университета. 2022. № 476. URL: https://cyberleninka.ru/article/n/biometricheskaya-identifikatsiya-v-internete-tendentsii-pravovogo-regulirovaniya-v-rossii-i-za-rubezhom/viewer (27.06.2025).

29. Лихачев В.В. Биометрия в праве: сравнительно-правовой анализ Административное и муниципальное право. 2019. № 11. – С. 1335–1349. DOI: 10.7256/2454-0595.2019.11.31096 URL: https://nbpublish.com/ammag/ (07.07.2025).

30. "Analyses of Section 503.001 – Capture or Use of Biometric Identifier, Tex. Bus. & Com. Code § 503.001 | Casetext." Casetext.com. URL: https://casetext.com (30.05.2025)

31. Текст GDPR на русском с комментариями и ссылками | GDPR-Text.com. URL: https://gdpr-text.com/ru/ (23.05.2025).

32. Белая О.В., Кицай Ю.А. Биометрические данные как средство идентификации и аутентификации человека: Российский и международный опыт. Право и практика. 2020. № 1. URL: https://cyberleninka.ru/article/n/biometricheskie-dannye-kak-sredstvo-identifikatsii-i-autentifikatsii-cheloveka-rossiyskiy-i-mezhdunarodnyy-opyt (18.06.2024).

33. "Ответственность за нарушение закона о персональных данных." URL: https://www.garant.ru/actual/persona/otvetstvennost/) (10.06.2025).

34. Фаллетти Э. Алгоритмическая дискриминация и защита неприкосновенности частной жизни // Journal of Digital Technologies and Law. 2023. № 1(2). – С. 387–420. URL: https://doi.org/10.21202/jdtl.2023.16 (18.07.2025).

35. Баланс между выгодой и приватностью при регулировании данных: как его ищут в разных странах. TAdviser.ru. URL: https://www.tadviser.ru/index.php/MDM_-_Master_Data_Management (23.07.2025).

36. "О персональных данных и их защите – ИПС 'Әділет.'" Adilet.zan.kz. URL: https://adilet.zan.kz (23.07.2024).

37. Идрышева С.К. О Цифровом кодексе Казахстана. Право и государство. 2022. № 3(96). – С. 72–87. DOI: 10.51634/2307-5201_2022_3_72 – URL: https://doi.org/10.51634/2307-5201_2022_3_72 (21.07.2025).

38. "Передача базы телефонных номеров. История одного тендера 'Казахтелекома.'" Радио Азаттык. URL: https://rus.azattyq.org/a/kazakhstan-numbers-base-transfer-history-of-a-tender-of-kazakhtelecom/31757577.html (15.06.2025).

39. История одного тендера "Казахтелекома." Радио Азаттык. URL: https://rus.azattyq.org/a/kazakhstan-numbers-base-transfer-history-of-a-tender-of-kazakhtelecom/31757577.html (15.06.2025).

40. Жулмухаметова Ж. Штраф за отказ от всеобщей дактилоскопии могут отменить. Zakon.kz. URL: https://www.zakon.kz/sobytiia/6408995-shtraf-za-otkaz-ot-vseobshchey-daktiloskopii-mogut-otmenit.html (14.03.2024).

41. Закон Республики Казахстан от 30 декабря 2016 г. № 40-VI «О дактилоскопической и геномной регистрации» (с изменениями и дополнениями по состоянию на 01.07.2021 г.) URL: https://online.zakon.kz/Document/?doc_id=33276266 (14.03.2024).

42. АИС БИЛ – Автоматизированная Информационная Система Биометрическая идентификация личности.

43. "Исследование возможных экономических, социальных и правовых последствий закона РК 'О дактилоскопической и геномной регистрации.'" Soros Kazakhstan Foundation, 23 June 2021. URL: https://www.soros.kz/ru/study-of-the-law-of-the-republic-of-kazakhstan-on-fingerprint-and-genomic-registration/ (14.05.2024).

44. "Защита персональных данных в Казахстане: статус, риски и возможности." Soros Kazakhstan Foundation, 29 Apr. 2020. URL: https://www.soros.kz/ru/protection-of-personal-data-in-kazakhstan-status-risks-and-opportunities/ (15.05.2024).

45. Утеген Д., Рахметов Б. Технология распознавания лиц и обеспечение безопасности биометрических данных: компаративный анализ моделей правового регулирования. Journal of Digital Technologies and Law. 2023. 1(3): 825–844. DOI: 10.21202/jdtl.2023.36

References:

1. Galiullina D.R. Biometricheskie personälnye danye. Dokument. Arhiv. İstoria. Sovremenöst. 2015. № 15. S. 264–268. URL: https://elar.urfu.ru/bitstream/10995/32968/1/dais-2015-15-22.pdf (07.06.2025).

2. Inc, Spiceworks. "Data Snapshot: Biometrics in the Workplace Commonplace, but Are They Secure?" The Spiceworks Community. URL: https://community.spiceworks.com/security/articles/2952-data-snapshot-biometrics-in-the-workplace-commonplace-but-are-they-secure/ (27.03.2025).

3. "Biometricheskie personälnye danye i tehnologii identifikasii: kakie pravovye problemy mogut vozniknüt?"

4. Helen D. Börba s terorizmom, sanksii i voina. International Review. 2021. №916–917. S. 805–846, URL: https://international-review.icrc.org/sites/default/files/reviews-pdf/2023-06/IRRC_916-917_RU_805-846_Katja_Lindskov_Jacobsen.pdf (27.03.2025).

5. Burt, Chris. "Global Biometrics Market Forecast to Surpass \$82 B by 2027 despite Pandemic | Biometric Update."14 Oct. 2020. URL: https://www.biometricupdate.com/202010/global-biometrics-market-forecast-to-surpass82b-by-2027-despite-pandemic (27.03.2025).

6. Salihov D.R. Pandemia i personälnye danye: kak rasprostranenie novoi koronavirusnoi infeksii brosaet novye vyzovy personälnym dannym // Konstitusionnoe i munisipälnoe pravo. 2021. № 3. – S. 46–50. URL: https://publications.hse.ru/articles/459709669 (09.06.2025).

7. "Biometric Data and COVID-19 in the Workplace." JD Supra. URL: https://www.jdsupra.com/legalnews/biometric-data-and-covid-19-in-the-86112/ (17.03.2025).

8. "Nasbank: V pilotnom rejime zapuşen servis sentra obmena identifikasionnymi dannymi." Delovoi portal Kapital.kz. URL: https://kapital.kz/tehnology/86517/natsbank-v-pilotnom-rezhime-zapushchen-servis-tsentra-obmena-identifikatsionnymi-dannymi.html (14.05.2025).

9. Postanovlenie Pravitelstva Respubliki Kazahstan ot 12 dekabrä 2017 g. № 827 «Ob utverjdenii Gosudarstvennoi programy "Sifrovoi Kazahstan"» (s izmeneniami i dopolneniami po sostoianiu na 01.10.2020 g.) URL: https://online.zakon.kz/Document/?doc_id=37168057 (14.03.2025).

10. Sbornik prakticheskih rekomendasi Organizasii Obedinennyh Nasi po otvetstvennomu ispölzovaniu biometricheskih dannyh i obmenu imi v ramkah börby s terorizmom. URL: https://www.unodc.org/pdf/terrorism/Compendium-Biometrics/_.pdf (26.04.2025).

11. 'V Rosii zarabotala edinaia gosudarstvennaia sistema biometrii' (Vedomosti, 30 Dec. 2021) URL: https://www.vedomosti.ru/society/news/2021/12/30/903427-putin-podpisal-zakon-o-biometrii (07.08.2025).

12. Department of Homeland Security. "Fusion Centers." Department of Homeland Security, 19 Sept. 2019. URL: https://www.dhs.gov/fusion-centers (23.05.2025).

13. Mify i opasenia: pochemu rosiane boiatsä biometrii. Legalacademy.ru. URL: https://legalacademy.ru/sphere/post/mify-i-opaseniya-pochemu-rossiyane-boyatsya-biometrii (31.07.2025).

14. Petrova D.A., İurtaev V.A. Unified Biometric System: Legal Regulation and Functions Problems. European Proceedings of Social and Behavioural Sciences. 2022. Vol. 139. – S. 712–719. DOI: 10.15405/epsbs.2022.06.84 URL: https://doi.org/10.15405/epsbs.2022.06.84.

15. Şilina S. Uglubläiäs v proşloe, razmyşläia o nastoiaşem i issleduia külturnye nüansy: Mnogogrannoe issledovanie biometricheskoi proverki lichnosti. İssledovatelski institut «Paradigma». 2024. – 58 s. URL: https://www.researchgate.net/publication/377974352_Delving_into_the_past_pondering_the_present_and_probing_cultural_nuances_The_multi-faceted_exploration_of_biometric_identity_verification (09.06.2025).

16. Considerations for Fusion Center and Emergency Operations Center Coordination Comprehensive Preparedness Guide (CPG) 502. URL: https://www.fema.gov/media-library/assets/documents/25907 (01.06.2025).

17. U.S. Department of Justice. "Privacy Act of 1974." Justice.gov, 17 July 2015. URL: https://www.justice.gov/opcl/privacy-act-1974 (02.06.2025).

18. "Biometric Information Privacy Act (BIPA)." ACLU of Illinois, 26 Apr. 2021. URL: https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa (30.03.2025).

19. The Capture or Use of Biometric Identifiers Act (CUBI). 15 Sept. 2021. URL: https://www.caseguard.com/articles/the-capture-or-use-of-biometric-identifiers-act-cubi (13.05.2025).

20. Primenenie zakona Tehasa o biometrii sosredotocheno na iskustvennom intelekte. Holland & Knight LLP, 10 noiabrä 2022 g. URL: https://www.hklaw.com/en/insights/publications/2022/11/texas-enforcement-of-biometric-law-focuses-on-artificial-intelligence (31.07.2025).

21. "California Consumer Privacy Act (CCPA)." Google Cloud. URL: https://cloud.google.com/security/compliance/ccpa (22.05.2025).

22. "Vlasti SŞA opolchilis na Facebook za nelegälnoe raspoznavanie lis pölzovatelei." CNews.ru. URL: https://www.cnews.ru/news/top/2022-02-25_vlasti_ssha_opolchilis_na (17.05.2025).

23. Nejafzade N., Kaşiani H. Face Image Quality Vector Assessment for Biometrics Applications. 2023 IEEE/CVF Winter Conference on Applications of Computer Vision Workshops (WACVW), SŞA. 2023. – S. 511–520. DOI: 10.1109/WACVW58289.2023.00057 URL: https://doi.org/10.1109/WACVW58289.2023.00057 (17.05.2025).

24. "V SŞA podan isk k Amazon, Google i Microsoft iz-za sbora konfidensiälnyh svedeni." RAPSİ. URL: https://rapsinews.ru/international_news/20200715/306034494.html (18.05.2025).

25. Biometrics Litigation: An Evolving Landscape | Practical Law. URL: https://content.next.westlaw.com/practical-law/document/Id18ae0a6f51711e598dc8b09b4f043e0/Biometrics-Litigation-An-Evolving-Landscape?viewType=FullText\&transitionType=Default\&contextData=(sc.Default) (14.07.2025).

26. Grei D., Sitron D. Razbitoe zerkalo: Podvodnye kamni i potensial mozaichnoi teorii privatnosti v ramkah Chetvörtoi popravki. North Carolina Journal of Law & Technology. 2013. T. 14, № 2. – S. 381. URL: https://scholarship.law.unc.edu/ncjolt/vol14/iss2/3/ (23.06.2025).

27. Determann L. Rukovodstvo po zakonodatelstvu o zaşite dannyh: Mejdunarodnoe korporativnoe sootvetstvie. 5-e izd. 2018. – 340 s.

28. Kuznesova S.S., Mochalov A.N., Salikov M.S. Biometricheskaia identifikasia v internete: tendensii pravovogo regulirovania v Rosii i za rubejom // Vestnik Tomskogo gosudarstvennogo universiteta. 2022. № 476. URL: https://cyberleninka.ru/article/n/biometricheskaya-identifikatsiya-v-internete-tendentsii-pravovogo-regulirovaniya-v-rossii-i-za-rubezhom/viewer (27.06.2025).

29. Lihachev V.V. Biometria v prave: sravnitelno-pravovoi analiz. Administrativnoe i munisipälnoe pravo. 2019. № 11. – S. 1335–1349. DOI: 10.7256/2454-0595.2019.11.31096 URL: https://nbpublish.com/ammag/ (07.07.2025).

30. "Analyses of Section 503.001 – Capture or Use of Biometric Identifier, Tex. Bus. & Com. Code § 503.001 | Casetext." Casetext.com. – URL: https://casetext.com (30.05.2025)

31. Teks GDPR na ruskom s komentariami i ssylkami | GDPR-Text.com. URL: https://gdpr-text.com/ru/ (23.05.2025).

32. Belaia O.V., Kisai Iu.A. Biometricheskie danye kak sredstvo identifikasii i autentifikasii cheloveka: Rosiski i mejdunarodnyi opyt. Pravo i praktika. 2020. № 1. URL: https://cyberleninka.ru/article/n/biometricheskie-dannye-kak-sredstvo-identifikatsii-i-autentifikatsii-cheloveka-rossiyskiy-i-mezhdunarodnyy-opyt (18.06.2024).

33. "Otvetstvenöst za naruşenie zakona o personälnyh dannyh." URL: https://www.garant.ru/actual/persona/otvetstvennost/) (10.06.2025).

34. Faletti E. Algoritmicheskaia diskriminasia i zaşita neprikosnovenosti chastnoi jizni // Journal of Digital Technologies and Law. 2023. № 1(2). – S. 387–420. URL: https://doi.org/10.21202/jdtl.2023.16 (18.07.2025).

35. Balans mejdu vygodoi i privatnöstü pri regulirovanii dannyh: kak ego işut v raznyh stranah. TAdviser.ru. URL: https://www.tadviser.ru/index.php/MDM_-_Master_Data_Management (23.07.2025).

36. "O personälnyh dannyh i ih zaşite – İPS 'Ädılet.'" Adilet.zan.kz. URL: https://adilet.zan.kz (23.07.2024).

37. İdryşeva S.K. O Sifrovom kodekse Kazahstana. Pravo i gosudarstvo. 2022. № 3(96). – S. 72–87. DOI: 10.51634/2307-5201_2022_3_72 – URL: https://doi.org/10.51634/2307-5201_2022_3_72 (21.07.2025).

38. “Peredacha bazy telefonnyh nomerov. İstoria odnogo tendera ‘Kazahtelekoma.’” Radio Azattyk. URL: https://rus.azattyq.org/a/kazakhstan-numbers-base-transfer-history-of-a-tender-of-kazakhtelecom/31757577.html (15.06.2025).

39. İstoria odnogo tendera “Kazahtelekoma.” Radio Azattyk. URL: https://rus.azattyq.org/a/kazakhstan-numbers-base-transfer-history-of-a-tender-of-kazakhtelecom/31757577.html (15.06.2025).

40. Julmuhametova J. Ştraf za otkaz ot vseobşei daktiloskopii mogut otmenit. Zakon.kz. URL: https://www.zakon.kz/sobytiia/6408995-shtraf-za-otkaz-ot-vseobshchey-daktiloskopii-mogut-otmenit.html (14.03.2024).

41. Zakon Respubliki Kazahstan ot 30 dekabrä 2016 g. № 40-VI «O daktiloskopicheskoi i genomnoi registrasii» (s izmeneniami i dopolneniami po sostoianiu na 01.07.2021 g.) URL: https://online.zakon.kz/Document/?doc_id=33276266 (14.03.2024).

42. AİS BİL – Avtomatizirovannaia İnformasionnaia Sistema Biometricheskaia identifikasia lichnosti.

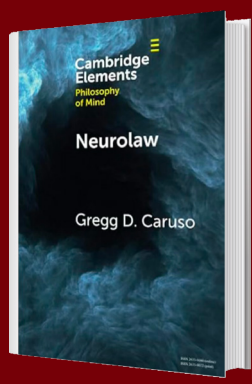
43. “İssledovanie vozmojnyh ekonomicheskih, sosiälnyh i pravovyh posledstvi zakona RK ‘O daktiloskopicheskoi i genomnoi registrasii.’” Soros Kazakhstan Foundation, 23 June 2021. URL: https://www.soros.kz/ru/study-of-the-law-of-the-republic-of-kazakhstan-on-fingerprint-and-genomic-registration/ (14.05.2024).

44. “Zaşita personälnyh dannyh v Kazahstane: status, riski i vozmojnosti.” Soros Kazakhstan Foundation, 29 Apr. 2020. URL: https://www.soros.kz/ru/protection-of-personal-data-in-kazakhstan-status-risks-and-opportunities/ (15.05.2024).

45. Utegen D., Rahmetov B. Tehnologia raspoznavania lis i obespechenie bezopasnosti biometricheskih dannyh: komparativnyi analiz modelei pravovogo regulirovania. Journal of Digital Technologies and Law. 2023. 1(3): 825–844. DOI: 10.21202/jdtl.2023.36

Для цитирования и библиографии: Утеген Д. Защита биометрических данных: анализ законодательства Казахстана в контексте зарубежной практики // Право и государство. № 4(109), 2025. – С. 31-42. DOI: 10.51634/2307-5201_2025_4_31

Материал поступил в редакцию 12.08.2025



НОВЫЕ КНИГИ

Gregg D. Caruso. Neurolaw (Elements in Philosophy of Mind). Publ.:Cambridge University Press, 2024. – 88 p.

ISBN-10: 1009271156
ISBN-13: 978-1009271158

Neurolaw is an area of interdisciplinary research on the meaning and implications of neuroscience for the law and legal practices. This Element addresses the potential contributions of neuroscience, and the brain sciences more generally, to criminal justice decision-making and policy. It distinguishes between three different areas and domains of investigation in neurolaw: assessment, intervention, and revision. The first concerns brain-based assessments, which may be used for predicting future violence, lie detection, judging legal insanity, and the like. The second concerns potential treatments and other interventions that aim at rehabilitating criminals and/or preventing crime before it occurs. The third investigates the ways that neuroscience may impact the law by changing or revising commonsense views about human nature and the causes of human action.