МРНТИ 10.19.61
УДК 342.72/.73
JEL K24

https://doi.org/10.46914/2959-4197-2026-1-3-285-299

ДЮСЕБАЕВ Ж.С.,*[1]
докторант.
*e-mail: z.dyussebayev@turan-edu.kz
ORCID ID: 0009-0009-5137-9835
РЕХСОН С.Н.,[1]
к.ю.н., ассоциированный профессор.
e-mail: s.rekhson@turan-edu.kz
ORCID ID: 0009-0009-4710-0387
САБЕРДИНОВА А.А.,[1]
м.ю.н., сениор-лектор.
e-mail: saberdinova@turan-edu.kz
ORCID ID: 0009-0007-5328-6443
КУДРЯВЦЕВА А.В.,[2]
д.ю.н., профессор.
e-mail: acifna@mail.ru
ORCID ID: 0000-0001-7666-8048
[1]Университет «Туран»,
г. Алматы, Казахстан
[2]Северо-Западный филиал
Российского государственного
университета правосудия им. В.М. Лебедева,
Санкт-Петербург, Россия

ИНСТИТУЦИОНАЛЬНЫЕ И ПРАВОВЫЕ МЕХАНИЗМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИСПОЛЬЗОВАНИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В РЕСПУБЛИКЕ КАЗАХСТАН: СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ С ЕВРОПЕЙСКОЙ МОДЕЛЬЮ

Аннотация

В статье проводится комплексный анализ институциональных и правовых механизмов защиты персональных данных при использовании технологий искусственного интеллекта (ИИ) в Республике Казахстан. Особое внимание уделяется сравнению с европейской моделью регулирования, в частности с Общим регламентом ЕС по защите данных (GDPR) и Регламентом об искусственном интеллекте (AI Act). Обоснована актуальность исследования в контексте масштабной цифровой трансформации Казахстана и реализации национальных стратегий в области ИИ. Цель работы – выявить правовые пробелы и противоречия между стимулированием инноваций в ИИ и гарантиями конфиденциальности личности. Методологической основой служат формально-юридический, сравнительно-правовой и институциональный подходы. Проанализированы ключевые нормативные акты Республики Казахстан, регулирующие отношения в сфере защиты персональных данных, цифровизации и искусственного интеллекта, а также действующие стратегические документы. Особое внимание уделено взаимосвязи правового регулирования персональных данных, цифровых технологий и искусственного интеллекта. Установлено, что казахстанское законодательство активно синхронизируется с европейскими стандартами, вводя рискориентированную модель регулирования ИИ с запретами на дискриминационные алгоритмы. Однако выявлены и пробелы: недостаточное внимание к предварительной оценке рисков ИИ-систем, ограниченность институционального надзора и права на объяснение автоматизированных решений. Результаты исследования актуальны для совершенствования нормативной базы Казахстана в области цифрового суверенитета, ИИ и защиты персональных данных.

Ключевые слова: искусственный интеллект, персональные данные, цифровой суверенитет, кибербезопасность, защита данных, регламент GDPR, законность обработки.

Введение

Интенсивное развитие цифровой экономики, электронного правительства и аналитических платформ принципиально изменило правовой режим персональных данных. Если в классическом понимании персональные данные выступали главным образом как сведения о частной жизни, подлежащие защите от неправомерного сбора, распространения или утечки, то в условиях алгоритмической обработки они одновременно превратились в материал для обучения моделей, профилирования, прогнозирования и последующего принятия решений, способных влиять на доступ человека к социальным благам, труду, кредиту, медицинским услугам и публичным сервисам.

Для Казахстана данная проблема имеет непосредственное конституционное значение. Конституция Республики Казахстан, принятая на республиканском референдуме 15 марта 2026 г., закрепляет человека, его жизнь, права и свободы в качестве высших ценностей государства. Особое значение для рассматриваемой проблематики имеет статья 21 Конституции, согласно которой каждому гарантируется право на неприкосновенность частной жизни, личную и семейную тайну, а также защита персональных данных от их незаконного сбора, обработки, хранения и использования, в том числе с применением цифровых технологий [1]. Тем самым защита персональных данных получила прямое конституционное закрепление не только как элемент охраны частной жизни, но и как самостоятельная гарантия в условиях цифровой трансформации.

Общий правовой режим сбора, обработки, хранения и защиты персональных данных в Республике Казахстан закреплен в специальном Законе «О персональных данных и их защите», который исходит из необходимости согласия субъекта, ограничения целей обработки и обеспечения конфиденциальности соответствующей информации [2].

Инфраструктурно-технологическая среда функционирования государственных и частных цифровых систем в настоящее время регулируется положениями Цифрового кодекса Республики Казахстан, устанавливающего правовые основы цифровизации, функционирования цифровых объектов и систем, использования цифровых данных и организации взаимодействия государства, граждан и организаций в цифровой среде [3].

Стратегический поворот к усилению киберустойчивости государства был закреплен в Концепции кибербезопасности Республики Казахстан («Киберщит Казахстана»), ориентированной на обеспечение устойчивости электронных информационных ресурсов и информационно-коммуникационной инфраструктуры [4]. В дальнейшем развитие искусственного интеллекта получило самостоятельное стратегическое оформление в Концепции развития искусственного интеллекта на 2024–2029 гг., утвержденной постановлением Правительства Республики Казахстан от 24 июля 2024 г. № 592 [5]. На современном этапе стратегическая рамка цифрового развития дополнена Общенациональной стратегией масштабной цифровизации и тотального внедрения технологий искусственного интеллекта «Digital Qazaqstan» до 2029 г., утвержденной Указом Президента Республики Казахстан от 9 июня 2026 г. № 1311. Стратегия определяет приоритеты дальнейшей цифровой трансформации и внедрения технологий искусственного интеллекта, что непосредственно связано с развитием правовых механизмов их безопасного и ответственного использования.

На официальном сайте уполномоченного министерства прямо указано, что в компетенцию профильного органа входят персональные данные и их защита, информационная безопасность, управление данными, электронное правительство и развитие ИИ, что делает институциональную архитектуру особенно важной для оценки конфликта между функциями стимулирования и контроля [6].

На уровне Европейского союза защита персональных данных в цифровой среде строится на сочетании общего и специального режимов. Базовым общим актом выступает GDPR, закрепляющий принципы законности, добросовестности, прозрачности, ограничения цели, минимизации данных, точности, ограничения хранения, целостности, конфиденциальности и подотчетности контролера [7]. Специальный секторный слой формирует AI Act, который вводит рискориентированную архитектуру регулирования ИИ, разграничивает запрещенные практики, высокорисковые системы, системы с обязанностями прозрачности и отдельный режим для моделей общего назначения [8]. Существенное значение для прикладного толкования статьи

25 GDPR имеют Руководящие принципы EDPB 4/2019 (The European Data Protection Board – Европейский совет по защите данных) о защите данных по проекту и по умолчанию, которые требуют встраивать защитные и минимизирующие решения в архитектуру продукта еще до ввода системы в эксплуатацию [9]. Международный контекст дополняется модернизированной Конвенцией 108+, закрепляющей межгосударственные стандарты автоматизированной обработки персональных данных и подтверждающей, что защита информации о личности является не исключительно национальным, а трансграничным правовым вопросом [10].

Современная научная литература исходит из того, что регулирование ИИ, защита данных и кибербезопасность образуют не изолированные, а взаимосвязанные контуры правового управления цифровыми рисками [11]. Особенно остро эта связь проявляется на стадии подготовки обучающих наборов, когда правовая проблема касается не только законности первичного сбора информации, но и последующего повторного использования данных для обучения модели, дообучения, валидации и применения выведенных из них прогнозов [12]. В результате возникает риск незаметной, но юридически значимой дискриминации: алгоритм может опираться на признаки, статистически коррелирующие с полом, возрастом, состоянием здоровья, социальным происхождением или этничностью, даже если эти признаки не названы открыто в модели [13]. Для преодоления такой асимметрии все большее значение приобретают процедуры оценки алгоритмического воздействия и документирования рисков до запуска системы, а не только санкции после наступления неблагоприятных последствий [14].

Данный подход согласуется с выводами отечественных исследователей, отмечающих, что распространение искусственного интеллекта сопровождается не только технологическими преимуществами, но и расширением рисков утечки, повторной идентификации и непреднамеренного выявления чувствительной информации. Умитчинова Б.А., Гаврилова Ю.А. и Мензюк Г.А. обращают внимание на недостаточную регламентацию автоматизированного принятия решений и отсутствие в казахстанском законодательстве полноценного механизма, обеспечивающего объяснимость решений, принятых с использованием ИИ. По мнению авторов, совершенствование регулирования должно быть направлено на усиление гарантий конфиденциальности и согласование национального законодательства с международными стандартами [27].

Актуальность настоящего исследования определяется тем, что Казахстан уже перешел к нормативному и институциональному этапу развития ИИ, однако пока не завершил переход к полноценной модели защиты персональных данных в высокорисковой алгоритмической среде. В национальном праве сохраняется разрыв между общими нормами о защите данных и специальными рисками автоматизированного принятия решений, алгоритмического вывода новых сведений, биометрической идентификации и непрозрачного профилирования. Проблема исследования заключается в том, что действующее законодательство Казахстана пока не дает однозначного ответа на ряд принципиальных вопросов: какие системы искусственного интеллекта следует относить к категории высокорисковых, в каких случаях необходимо проводить предварительную оценку их воздействия, каким должен быть объем обоснования принятого с их использованием решения, в каких формах должен осуществляться контроль и пересмотр таких решений человеком, а также на кого должна возлагаться ответственность за вред, причиненный в результате ошибочной или дискриминационной работы алгоритма.

Объектом исследования являются общественные отношения, возникающие в процессе создания, внедрения и использования ИИ-систем, обрабатывающих персональные данные физических лиц в Республике Казахстан. Предметом исследования выступают нормы национального и европейского права, официальные стратегии, механизмы надзора, права субъектов данных и обязанности операторов, разработчиков и поставщиков ИИ-систем. Цель статьи – определить степень достаточности институциональных и правовых механизмов защиты персональных данных при использовании искусственного интеллекта в Республике Казахстан и выработать предложения по их совершенствованию с учетом европейской модели. Для достижения цели поставлены следующие задачи: раскрыть характер рисков, которые ИИ создает для персональных данных; проанализировать казахстанское законодательство и институциональную архитектуру; исследовать конструкцию GDPR и AI Act; сопоставить национальные и европейские подходы к оценке воздействия и классификации риска; определить пробелы национального регулирования; предложить модель правового и институционального усиления защиты данных.

Гипотеза исследования заключается в том, что эффективная защита персональных данных в эпоху ИИ невозможна исключительно на основе общих правил согласия, хранения и конфиденциальности; она требует специальной рискориентированной модели, включающей оценку воздействия, алгоритмический аудит, объяснение значимых решений и автономный надзор.

Материалы и методы

Материальную основу исследования составили акты национального и европейского права, официальные стратегические документы, разъясняющие материалы уполномоченных органов и современные научные публикации, посвященные регулированию ИИ и защите персональных данных. Национальный массив источников был сформирован из Конституции Республики Казахстан, Закона Республики Казахстан «О персональных данных и их защите», Цифрового кодекса Республики Казахстан от 9 января 2026 г. № 255-VIII ЗРК, Концепции кибербезопасности «Киберщит Казахстана», Концепции развития искусственного интеллекта на 2024–2029 гг., а также официальных сведений и документов уполномоченных государственных органов [6]. Европейский нормативный массив включал GDPR, AI Act, официальные руководства EDPB и документы Совета Европы по Конвенции 108+ [7–10].

Научная база отбиралась по критериям релевантности теме, академической рецензируемости, новизны и пригодности для сравнительно-правового анализа. В основу положены статьи 2021–2024 гг. из Scopus и Web of Science, исследующие регуляторную конкуренцию в сфере ИИ, рискориентированное регулирование, объяснимость, подотчетность, аудит и соотношение продуктовой безопасности с фундаментальными правами. В частности, N.A. Smuha показывает, что развитие законодательства об ИИ происходит в логике глобальной регуляторной конкуренции, где государство должно одновременно обеспечивать защиту прав и технологическое развитие [15]. M. Veale и F. Zuiderveen Borgesius подчеркивают, что анализ AI Act должен строиться не только на тексте проекта или регламента, но и на оценке того, какие реальные механизмы контроля и исполнения способен породить рискориентированный подход [16].

Методологическую основу исследования составили формально-юридический, сравнительно-правовой, системный, институциональный и нормативно-аналитический методы. Формально-юридический метод использовался для выявления содержания действующих правовых норм: прав субъектов данных, обязанностей операторов, требований к безопасности, прозрачности и человеческому участию в ИИ-системах. Сравнительно-правовой метод позволил сопоставить Казахстан и Европейский союз по единым функциональным критериям: наличие классификации высокорисковых систем, обязательств по оценке воздействия, прав на объяснение, институционального надзора, санкций и средств правовой защиты. Системный метод дал возможность рассмотреть защиту персональных данных как часть более широкой цифровой архитектуры, включающей кибербезопасность, цифровой суверенитет и управление государственными платформами. Институциональный метод применялся для анализа распределения полномочий между органами цифрового развития, органами по защите данных и иными субъектами контроля. Нормативно-аналитический метод использовался для формулирования предложений de lege ferenda (с точки зрения совершенствования законодательства) по адаптации отдельных элементов европейской модели к правовой системе Казахстана.

Исследование носит доктринально-правовой характер и не включает собственные социологические опросы либо статистическое моделирование. Его задача состоит не в измерении распространенности нарушений, а в выявлении достаточности или недостаточности существующих юридических механизмов. Надежность выводов обеспечивалась триангуляцией источников: значимые положения проверялись одновременно по нормативному тексту, официальному институциональному документу и научной публикации.

Результаты и обсуждение

Персональные данные как ресурс обучения и фактор алгоритмического воздействия.

Первый результат исследования состоит в том, что ИИ радикально меняет функциональное значение персональных данных. Данные перестают быть лишь объектом пассивного хранения

и становятся активным ресурсом обучения, настройки и функционирования алгоритма. При этом правовое значение имеют не только изначально предоставленные сведения, но и новые характеристики, выведенные моделью: риск-профили, предикторы поведения, чувствительности, платежеспособности, надежности и пригодности к тому или иному решению. Формально это означает, что права субъекта должны распространяться не исключительно на первичный набор сведений, но и на алгоритмически созданные производные характеристики, если они относятся к определенному или определяемому лицу [12].

Другая принципиальная проблема заключается в том, что формальное наличие человека в цепочке принятия решения еще не гарантирует справедливости и правовой защиты. R. Binns убедительно показывает, что «человек в контуре» превращается в фикцию, если лицо, принимающее итоговое решение, не понимает ограничений алгоритма, не располагает достаточной информацией о его выходных данных и не имеет реальной возможности отменить либо исправить результат [17]. Из этого следует, что участие человека в пересмотре решения не должно носить формальный характер, а должно обеспечивать реальную возможность критической оценки рекомендации, сформированной алгоритмом.

Риск дискриминации в ИИ-системах проявляется не только через прямое использование чувствительных категорий данных, но и через коррелирующие признаки. J. Adams-Prassl, R. Binns и A. Kelly-Lyth показывают, что алгоритм может прямо или косвенно дискриминировать даже тогда, когда применяет, казалось бы, нейтральные данные – геолокацию, историю потребления, особенности цифрового поведения или образовательный трек, выступающие заменителями защищаемых характеристик [18]. Следовательно, правовой контроль качества обучающих данных должен включать не только проверку точности и полноты, но и анализ структурной предвзятости, репрезентативности и потенциальной непрямой дискриминации.

Из этого вытекает базовый вывод: защита персональных данных в эпоху ИИ не может ограничиваться безопасностью базы данных и получением согласия. Она должна охватывать весь жизненный цикл ИИ-системы: постановку цели, сбор и отбор данных, обучение модели, тестирование, внедрение, эксплуатацию, последующий мониторинг и прекращение использования.

Сильные стороны и пробелы казахстанской модели

Второй результат исследования состоит в том, что в Казахстане уже создана базовая нормативная основа защиты персональных данных в цифровой среде, однако она еще не трансформирована в полноценную ИИ-ориентированную модель. Сильной стороной национального регулирования является наличие конституционных гарантий, специального законодательства о защите персональных данных, комплексного регулирования цифровой среды в рамках Цифрового кодекса Республики Казахстан, стратегической линии развития кибербезопасности и концептуального документа по развитию искусственного интеллекта [1–5]. Это означает, что правовой вакуум в Казахстане отсутствует: обработка данных в ИИ-системах уже подпадает под существующий правовой режим.

Одновременно исследование выявило ряд системных пробелов. Во-первых, действующие нормы недостаточно четко различают обычную цифровую обработку и высокорисковую алгоритмическую обработку. Законодательство пока не предлагает общей классификации ИИ-систем по уровню риска для прав и свобод личности. Между тем одна и та же технология может использоваться в справочном сервисе с минимальным риском либо в кредитном скоринге, социальной помощи, правоохранительной идентификации или профилировании уязвимых групп, где последствия для человека многократно выше.

Во-вторых, в национальном праве пока отсутствует универсальный механизм, функционально эквивалентный европейской DPIA (Data Protection Impact Assessment – Оценка воздействия на защиту данных). Да, ИИ-системы могут подпадать под требования информационной безопасности, ведомственного контроля и внутреннего комплаенса, однако ни одна из этих процедур не заменяет полноценную предварительную оценку воздействия на права человека. Поэтому модель остается преимущественно реактивной: нарушение обычно фиксируется уже после жалобы, инцидента или негативного эффекта.

Сходная проблематика выявлена и в современной казахстанской научной литературе. Кусаинова А.К. отмечает, что действующее законодательство Республики Казахстан не в полной мере отвечает современным вызовам цифровой обработки данных, в том числе вследствие

отсутствия надлежащих механизмов оценки воздействия на защиту персональных данных, а также недостаточной регламентации обработки биометрических и поведенческих данных. Автор связывает дальнейшее развитие национальной системы защиты данных с переходом к комплексной рискориентированной модели регулирования и внедрением процедуры DPIA [28].

В-третьих, законодательство Казахстана недостаточно четко регулирует право субъекта на получение объяснения причин принятия значимого автоматизированного решения. Действующее регулирование предусматривает право на информацию об обработке персональных данных. Однако этого недостаточно, когда необходимо установить причины отказа в предоставлении услуги, повышения кредитного риска, снижения приоритетности заявки или формирования неблагоприятного поведенческого профиля. В отношении решений, принимаемых с использованием систем искусственного интеллекта, целесообразно установить дополнительные требования. Оператор должен раскрывать роль алгоритма в принятии решения, основные виды использованных данных и факторы, повлиявшие на результат. Также необходимо предусмотреть возможность пересмотра решения человеком и порядок его обжалования.

Выявленная проблема получила отражение и в отечественной научной литературе. Умитчинова Б.А., Гаврилова Ю.А. и Мензюк Г.А. указывают, что действующее регулирование Казахстана не обеспечивает в достаточной степени право лица на получение объяснения при принятии решений с использованием искусственного интеллекта. Авторы связывают данный пробел с необходимостью дальнейшего развития правовых гарантий автоматизированной обработки персональных данных и повышения прозрачности алгоритмических решений [27].

В-четвертых, национальная институциональная модель характеризуется концентрацией цифровых, ИИ- и данных-компетенций в одном министерском контуре [6]. Подобная централизация может быть удобна для координации цифровой трансформации, однако она одновременно повышает риск конфликта между задачей ускоренного внедрения технологий и задачей строгого ограничения их неправомерного либо чрезмерного применения. Из этого не следует, что Казахстан обязательно должен механически создавать полностью новый независимый орган по модели ЕС. Однако функциональное разделение стимулирующих и контрольных полномочий необходимо, особенно применительно к высокорисковым системам.

Наконец, существенным пробелом остается правовой режим биометрии и поведенческих данных. Не всякая ИИ-обработка влечет одинаковый риск, но биометрическая идентификация, удаленное распознавание, категоризация и распознавание эмоций требуют усиленного контроля. В национальном праве такие операции пока не разведены на достаточном уровне детализации, что создает риск слишком широкого усмотрения при их внедрении в государственном и частном секторе.

Отдельного внимания заслуживает правовой режим биометрических и поведенческих данных. Как отмечает Кусаинова А.К., именно данные категории требуют дополнительного нормативного внимания в связи с отсутствием достаточной детализации условий их обработки и контроля за рисками для прав субъектов данных [28].

Европейская модель как функциональный ориентир для Казахстана

Третий результат исследования состоит в том, что европейская модель не должна рассматриваться как готовый текст для копирования, но представляет собой ценный набор функциональных институтов, пригодных для адаптации. M. Almada и N. Petit обоснованно характеризуют AI Act как гибридную правовую конструкцию, в которой сочетаются логика безопасности продукции и логика защиты фундаментальных прав [19]. Для Казахстана это означает необходимость выйти за рамки чисто технической надежности ИИ и признать, что вопрос законности становится вопросом воздействия на достоинство, равенство, автономию и эффективную правовую защиту человека.

Особое значение имеет сочетание двух оценочных процедур. A. Mantelero показывает, что фундаментально-правовая оценка воздействия, предусмотренная AI Act, по своей природе шире, чем традиционная оценка воздействия на защиту данных, поскольку охватывает не только приватность, но и не дискриминацию, доступ к услугам, права ребенка и иные фундаментальные права [20]. Следовательно, при адаптации европейской модели Казахстану следует не просто копировать термин DPIA, а вводить двухуровневую процедуру: оценку воздействия на персональные данные и оценку более широкого правового риска в высокорисковых ИИ-системах.

С точки зрения институциональной подотчетности важным ориентиром является подход C. Novelli, M. Taddeo и L. Floridi, согласно которому подотчетность в ИИ невозможна без четкого распределения обязанностей между участниками жизненного цикла системы, наличия механизма объяснения, документирования и возможности внешней проверки [21]. Иными словами, ответственность не должна растворяться между программистом, поставщиком данных, интегратором, госорганом и конечным пользователем системы. Для высокой правовой определенности Казахстану необходимо закрепить принцип: ответственность следует за фактическим контролем над соответствующим этапом ИИ-системы.

Важна и координация права ИИ с кибербезопасностью. F. Casarosa указывает, что несогласованность между режимами сертификации кибербезопасности и регулированием ИИ способна породить лакуны, при которых система формально безопасна как цифровой продукт, но при этом не проходит достаточной проверки с точки зрения прав личности [22]. Для Казахстана это особенно актуально, поскольку национальная цифровая политика исторически развивалась через логику информационной безопасности и устойчивости инфраструктуры.

Следующий функциональный элемент европейской модели связан с трансграничным измерением. C. Peukert, S. Bechtold, M. Batikas и T. Kretschmer показывают, что GDPR обладает экстерриториальным и экспортирующим эффектом: компании за пределами ЕС зачастую подстраивают практики работы с данными под европейские стандарты, поскольку это снижает трансакционные издержки и облегчает участие в трансграничных рынках [23]. Для Казахстана это означает, что сближение с европейскими стандартами выгодно не только с точки зрения прав человека, но и с точки зрения конкурентоспособности цифровых сервисов.

При этом, как подчеркивают J. Laux, S. Wachter и B. Mittelstadt, ни доверие пользователей, ни политическая риторика об «этичном ИИ» не могут подменить юридическую оценку допустимости риска [24]. Поэтому правовой режим должен строиться не на декларациях о полезности технологии, а на проверяемых критериях необходимости, соразмерности, качества данных, человеческого контроля и возможности оспаривания.

Практическое значение европейской правоприменительной линии особенно хорошо видно на примере дела SCHUFA (Schutzgemeinschaft für Absatzfinanzierung – немецкое кредитное бюро). Суд ЕС признал, что автоматизированный кредитный рейтинг способен рассматриваться как решение, подпадающее под сферу статьи 22 GDPR, если организация придает ему определяющее значение при заключении, исполнении или отказе в договоре [25]. Для Казахстана это означает, что формальное участие сотрудника в принятии окончательного решения само по себе не исключает применения повышенных требований к защите прав субъекта. Если фактический результат определяется алгоритмической оценкой, наличие последующего одобрения со стороны человека не должно рассматриваться как достаточное основание для исключения такой системы из соответствующего правового режима.

Не менее важное значение для Казахстана имеет подход, сформулированный Судом ЕС в деле Schrems II (C-311/18). Поводом для рассмотрения дела стала передача компанией Facebook Ireland персональных данных пользователей в США. Максимилиан Шремс оспаривал такую передачу, указывая на недостаточный уровень защиты данных от доступа со стороны государственных органов США. В 2020 г. Суд ЕС признал недействительным решение о механизме EU–US Privacy Shield, при этом подтвердив возможность использования стандартных договорных положений при условии оценки фактического уровня защиты данных в стране их получения. Таким образом, Суд ЕС исходил из того, что наличие формальных договорных гарантий само по себе не обеспечивает надлежащую защиту персональных данных. Необходимо учитывать также законодательство и практику его применения в государстве, в которое передаются данные. Для Казахстана данный подход имеет значение при регулировании трансграничной передачи персональных данных, особенно в случаях их передачи в юрисдикции с иным уровнем правовой защиты. [26].

Использование зарубежных облачных сервисов и глобальных моделей искусственного интеллекта может предполагать передачу персональных данных за пределы Казахстана. Поэтому необходим усиленный контроль за такой трансграничной передачей, особенно при использовании ИИ-систем в государственных и квазигосударственных организациях и при обработке данных в системах с высоким уровнем риска.

Таблица 1 – Сравнительная таблица Казахстана и Европейского союза

Аспект	Республика Казахстан	Европейский союз	Сравнительный вывод
Базовые правовые акты	Конституция Республики Казахстан: принята на республиканском референдуме 15 марта 2026 г.; Закон Республики Казахстан от 21 мая 2013 г. № 94-V «О персональных данных и их защите»; Цифровой кодекс Республики Казахстан от 9 января 2026 г. № 255-VIII ЗРК; постановление Правительства Республики Казахстан от 30 июня 2017 г. № 407 «Об утверждении Концепции кибербезопасности («Киберщит Казахстана»)»; постановление Правительства Республики Казахстан от 24 июля 2024 г. № 592 «Об утверждении Концепции развития искусственного интеллекта на 2024–2029 гг.».	Регламент (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных (GDPR); Регламент (ЕС) 2024/1689 Европейского парламента и Совета от 13 июня 2024 г., устанавливающий согласованные правила в области искусственного интеллекта (AI Act); руководящие документы Европейского комитета по защите данных (EDPB); Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, измененная Протоколом CETS № 223 (Convention 108+).	В Казахстане уже есть базовый каркас, но нет столь же детализированной ИИ-специфики, как в ЕС
DPIA/эквиваленты	Универсальный обязательный механизм DPIA для высокорисковых ИИ-систем не сформирован.	GDPR требует DPIA по статье 35; AI Act требует fundamental rights impact assessment для ряда deployers.	Казахстану нужен обязательный двухуровневый механизм оценки риска.
Институциональные органы	Профильное министерство совмещает ИИ, данные, инфобез и цифровое развитие.	Национальные DPA, EDPB, AI Office, органы рыночного надзора	В ЕС контроль институционально более дифференцирован.
Классификация высокорисковых систем	Фрагментарная, без законченной общей градации.	Запрещенные практики, high-risk AI systems, transparency obligations, GPAI.	Казахстану требуется материализованная классификация риска.
Полномочия по принуждению	Существуют общие механизмы административного контроля и защиты данных, но отсутствует завершенный режим именно для ИИ.	Conformity assessment, registration, market surveillance, corrective measures, substantial fines.	В ЕС enforcement-функция развита значительно глубже.
Средства правовой защиты	Общие жалобы, административное и судебное обжалование, защита прав субъектов данных по общим правилам.	Жалоба в DPA, судебная защита, компенсация, объяснение значимого решения, специальные гарантии статьи 22 GDPR.	Казахстану необходимо специальное право на объяснение и пересмотр ИИ-решения.
Примечание: Составлено авторами на основе анализа источников [1–10].			

Предлагаемая модель реформирования национального регулирования

На основании проведенного анализа предлагается комплексная национальная модель, состоящая из взаимосвязанных материальных и процессуальных элементов.

Во-первых, Закон «О персональных данных и их защите» следует дополнить специальным разделом об ИИ-обработке персональных данных. В нем необходимо определить понятия ав-

томатизированного решения, профилирования, алгоритмически выведенных данных, высокорисковой обработки, человеческого пересмотра и алгоритмического аудита.

Во-вторых, требуется закрепить обязательную оценку воздействия для высокорисковых ИИ-систем. Такая оценка должна проводиться до ввода системы в эксплуатацию и включать: описание цели, правового основания и контекста использования; перечень категорий данных и их источников; оценку необходимости и соразмерности; анализ риска для частной жизни, равенства и недискриминации; проверку качества и репрезентативности данных; описание человеческого контроля; механизм исправления ошибок и рассмотрения жалоб; меры минимизации риска; решение о допустимости внедрения.

В-третьих, необходима законодательно закрепленная классификация риска. Казахстану целесообразно выделить: запрещенные практики; высокорисковые системы; системы со специальными обязанностями прозрачности; системы общего и низкого риска. Отнесение к высокому риску должно определяться не по абстрактному названию технологии, а по сочетанию критериев: чувствительность данных, масштаб обработки, использование биометрии, влияние на права и услуги, уязвимость затрагиваемых групп, возможность дискриминации и сложность эффективного обжалования.

В-четвертых, следует закрепить специальное право субъекта данных на объяснение значимого решения. Лицо, в отношении которого принято решение с использованием ИИ-системы, порождающее юридические последствия либо сопоставимо существенно влияющее на его права и законные интересы, должно иметь право получить ясное объяснение роли ИИ, основных категорий использованных данных, ключевых факторов результата, наличия человеческого участия, способа исправления ошибок и порядка пересмотра решения компетентным должностным лицом.

В-пятых, необходим обязательный правовой режим алгоритмического аудита. Для низкорисковых систем допустим внутренний аудит, но для высокорисковых государственных и квазигосударственных систем должен быть установлен внешний независимый аудит, проводимый до запуска, периодически в ходе эксплуатации и после существенного изменения модели либо цели обработки. Аудит должен охватывать не только техническую устойчивость системы, но и соблюдение правовых требований, отсутствие дискриминационных последствий, соответствие заявленным целям, полноту документации и эффективность механизмов обжалования.

В-шестых, требуется институциональное усиление надзора. Независимо от окончательной организационной модели в казахстанской системе должно быть обеспечено функциональное разграничение между продвижением ИИ и контролем за защитой персональных данных в ИИ-среде. Система контроля за использованием таких технологий должна предусматривать возможность проведения проверок, запроса необходимой документации и аудиторских материалов, а также приостановления использования системы при выявлении высокого и неустраненного риска.

В-седьмых, следует закрепить дифференцированный режим биометрических и поведенческих данных. Закон должен отличать биометрическую аутентификацию от удаленной идентификации, категоризации и распознавания эмоций. Необходимо установить перечень запрещенных практик, режим обязательной оценки воздействия для высокорискового биометрического применения и особый порядок использования таких систем в публичном секторе.

В-восьмых, требуется усилить регулирование трансграничной передачи данных в контексте ИИ. Передача данных иностранным ИИ-провайдерам должна сопровождаться оценкой уровня защиты в юрисдикции получателя, договорными ограничениями на вторичное использование данных и обучение модели для несогласованных целей, контролем субподрядчиков, правилами удаления и механизмом внепланового аудита.

В-девятых, целесообразно ввести публичный реестр высокорисковых ИИ-систем, используемых государственными органами. Такой реестр должен содержать сведения о назначении системы, операторе, правовом основании, категориях обрабатываемых данных, факте проведения оценки воздействия, наличии аудита и процедурах обращения граждан.

В-десятых, внедрение новых технологий искусственного интеллекта должно осуществляться поэтапно и под постоянным контролем со стороны уполномоченных органов. Прове-

дение экспериментального тестирования не должно освобождать разработчиков и операторов от соблюдения требований законодательства о защите персональных данных. До начала использования системы необходимо оценить возможные риски для прав и свобод граждан, ограничить круг обрабатываемых данных и определить порядок контроля за ее работой. Решения, способные существенно затронуть права или законные интересы гражданина, не должны приниматься исключительно на основании результата автоматизированной обработки и должны предусматривать возможность их рассмотрения человеком.

Заключение

Проведенное исследование подтверждает заявленную гипотезу: эффективная защита персональных данных в условиях использования искусственного интеллекта требует перехода от классической модели охраны баз данных и согласия субъекта к модели управления алгоритмическим риском на всем жизненном цикле ИИ-системы. Казахстан уже располагает прямой конституционной основой защиты персональных данных в цифровой среде: статья 21 Конституции Республики Казахстан от 15 марта 2026 г. закрепляет защиту персональных данных от их незаконного сбора, обработки, хранения и использования, в том числе с применением цифровых технологий [1]. Вместе с тем наличие конституционной гарантии само по себе не устраняет необходимость дальнейшей детализации специальных процедур управления рисками, обеспечения прозрачности алгоритмических решений, распределения ответственности и эффективного контроля за использованием систем искусственного интеллекта.

Европейская модель важна для Казахстана прежде всего как набор функциональных институтов, а не как текст, подлежащий механическому заимствованию. Для национального законодательства наибольший интерес представляют: принцип подотчетности; защита данных по проекту и по умолчанию; обязательная оценка воздействия; обязательный человеческий пересмотр значимого решения; правовой режим внешнего аудита для высокорисковых систем; рискориентированная классификация ИИ-систем; особые правила биометрической идентификации; усиленный контроль трансграничной передачи данных.

Практическое значение статьи состоит в том, что предлагаемые выводы могут быть использованы при совершенствовании Закона Республики Казахстан «О персональных данных и их защите», а также при разработке подзаконных нормативных правовых актов, регулирующих использование высокорисковых систем искусственного интеллекта, разработке процедур аудита и оценки воздействия, а также при институциональном усилении органов, ответственных за контроль над обработкой персональных данных в цифровой среде. Научный вклад исследования выражается в интеграции казахстанской и европейской проблематики в единую сравнительно-правовую рамку, позволяющую показать, что защита персональных данных в эпоху ИИ – это уже не узкий вопрос конфиденциальности, а самостоятельный институт цифрового конституционализма, подотчетности и правовой устойчивости государства.

ЛИТЕРАТУРА

1 Конституция Республики Казахстан: принята на республиканском референдуме 15 марта 2026 года // ИПС «Әділет». – 2026. URL: https://adilet.zan.kz/rus/docs/K2600000000 (дата обращения: 04.09.2026).

2 Закон Республики Казахстан «О персональных данных и их защите» от 21 мая 2013 года № 94-V // ИПС «Әділет». – 2026. URL: https://adilet.zan.kz/rus/docs/Z1300000094 (дата обращения: 13.07.2026).

3 Цифровой кодекс Республики Казахстан: Кодекс Республики Казахстан от 9 января 2026 года № 255-VIII ЗРК // ИПС «Әділет». – 2026. URL: https://adilet.zan.kz/rus/docs/K2600000255 (дата обращения: 13.07.2026).

4 Об утверждении Концепции кибербезопасности («Киберщит Казахстана»): постановление Правительства Республики Казахстан от 30 июня 2017 года № 407 // ИПС «Әділет». – 2026. URL: https://adilet.zan.kz/rus/docs/P1700000407 (дата обращения: 13.07.2026).

5 Об утверждении Концепции развития искусственного интеллекта на 2024–2029 годы: постановление Правительства Республики Казахстан от 24 июля 2024 года № 592 // ИПС «Әділет». – 2026. URL: https://adilet.zan.kz/rus/docs/P2400000592 (дата обращения: 13.07.2026).

6 Министерство искусственного интеллекта и цифрового развития Республики Казахстан: официальный сайт. URL: https://www.gov.kz/memleket/entities/maidd?lang=ru (дата обращения: 13.07.2026).

7 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) // Official Journal of the European Union. 2016. L 119. P. 1–88. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed: 13.07.2026).

8 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) // Official Journal of the European Union. 2024. OJ L, 2024/1689. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (accessed: 13.07.2026).

9 European Data Protection Board. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. Version 2.0. Brussels, 2020. URL: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en (accessed: 13.07.2026).

10 Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. CETS No. 223. Strasbourg, 2018. URL: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=223 (accessed: 13.07.2026).

11 Andraško J., Mesarčík M., Hamuľák O. The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework // AI & Society. 2021. Vol. 36. No. 2. P. 623–636.

12 Hacker P. A legal framework for AI training data: from first principles to the Artificial Intelligence Act // Law, Innovation and Technology. 2023. Vol. 15. No. 2. P. 257–301.

13 Wachter S., Mittelstadt B., Russell C. Why fairness cannot be automated: bridging the gap between EU non-discrimination law and AI // Computer Law & Security Review. 2021. Vol. 41. Article 105567.

14 Kaminski M.E., Malgieri G. Algorithmic impact assessments under the GDPR: producing multi-layered explanations // International Data Privacy Law. 2021. Vol. 11. No. 2. P. 125–144.

15 Smuha N.A. From a "race to AI" to a "race to AI regulation": regulatory competition for artificial intelligence // Law, Innovation and Technology. 2021. Vol. 13. No. 1. P. 57–84.

16 Veale M., Zuiderveen Borgesius F. Demystifying the Draft EU Artificial Intelligence Act: analysing the good, the bad, and the unclear elements of the proposed approach // Computer Law Review International. 2021. Vol. 22. No. 4. P. 97–112.

17 Binns R. Human judgment in algorithmic loops: individual justice and automated decision-making // Regulation & Governance. 2022. Vol. 16. No. 1. P. 197–211.

18 Adams-Prassl J., Binns R., Kelly-Lyth A. Directly discriminatory algorithms // The Modern Law Review. 2023. Vol. 86. No. 1. P. 144–175.

19 Almada M., Petit N. The EU AI Act: between product safety and fundamental rights // Common Market Law Review. 2024. Vol. 61. No. 3. P. 655–696.

20 Mantelero A. The Fundamental Rights Impact Assessment in the AI Act: roots, legal obligations and key elements for a model template // Computer Law & Security Review. 2024. Vol. 54. Article 105980.

21 Novelli C., Taddeo M., Floridi L. Accountability in artificial intelligence: what it is and how it works // AI & Society. 2024. Vol. 39. P. 1871–1882.

22 Casarosa F. Cybersecurity certification of Artificial Intelligence: a missed opportunity to coordinate between the Artificial Intelligence Act and the Cybersecurity Act // International Cybersecurity Law Review. 2022. Vol. 3. P. 5–32.

23 Peukert C., Bechtold S., Batikas M., Kretschmer T. Regulatory export and spillovers: how GDPR affects global markets for data // Management Science. 2022. Vol. 68. No. 4. P. 3186–3204.

24 Laux J., Wachter S., Mittelstadt B. Trustworthy artificial intelligence and the European Union AI Act: on the conflation of trustworthiness and acceptability of risk // Regulation & Governance. 2024. Vol. 18. No. 1. P. 3–32.

25 Judgment of the Court of Justice of the European Union of 7 December 2023, OQ v Land Hessen, Case C-634/21, ECLI:EU:C:2023:957. URL: https://curia.europa.eu/juris/liste.jsf?num=C-634/21 (accessed: 13.07.2026).

26 Judgment of the Court of Justice of the European Union of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, Case C-311/18, ECLI:EU:C:2020:559. URL: https://curia.europa.eu/juris/liste.jsf?num=C-311/18 (accessed: 13.07.2026).

27 Умитчинова Б.А., Гаврилова Ю.А., Мензюк Г.А. Правовое регулирование персональных данных в условиях развития искусственного интеллекта: зарубежный опыт и вызовы для Казахстана // Вестник Института законодательства и правовой информации Республики Казахстан. 2025. № 3 (80). С. 37–53. DOI: 10.52026/2788-5291_2025_80_3_37

28 Кусаинова А.К. Проблемы правового регулирования и перспективы совершенствования законодательства Республики Казахстан в сфере защиты персональных данных // Veritas Legis Journal. 2026. Т. 2. № 2. DOI: 10.62687/VLJ.2.2.2026.50.

REFERENCES

1 Konstitucija Respubliki Kazahstan: prinjata na respublikanskom referendume 15 marta 2026 goda // IPS «Adilet». 2026. URL: https://adilet.zan.kz/rus/docs/K2600000000 (data obrashhenija: 04.09.2026) (In Russian)

2 Zakon Respubliki Kazahstan «O personal'nyh dannyh i ih zashhite» ot 21 maja 2013 goda No. 94-V // IPS «Ədilet». 2026. URL: https://adilet.zan.kz/rus/docs/Z1300000094 (data obrashhenija: 13.07.2026) (In Russian)

3 Cifrovoj kodeks Respubliki Kazahstan: Kodeks Respubliki Kazahstan ot 9 janvarja 2026 goda No. 255-VIII ZRK // IPS «Adilet». 2026. URL: https://adilet.zan.kz/rus/docs/K2600000255 (data obrashhenija: 04.09.2026) (In Russian)

4 Ob utverzhdenii Koncepcii kiberbezopasnosti («Kibershhit Kazahstana»): postanovlenie Pravitel'stva Respubliki Kazahstan ot 30 ijunja 2017 goda No. 407 // IPS «Ədilet». 2026. URL: https://adilet.zan.kz/rus/docs/P1700000407 (data obrashhenija: 13.07.2026) (In Russian)

5 Ob utverzhdenii Koncepcii razvitija iskusstvennogo intellekta na 2024–2029 gody: postanovlenie Pravitel'stva Respubliki Kazahstan ot 24 ijulja 2024 goda No. 592 // IPS «Ədilet». 2026. URL: https://adilet.zan.kz/rus/docs/P2400000592 (data obrashhenija: 13.07.2026) (In Russian)

6 Ministerstvo iskusstvennogo intellekta i cifrovogo razvitija Respubliki Kazahstan: oficial'nyj sajt. URL: https://www.gov.kz/memleket/entities/maidd?lang=ru (data obrashhenija: 13.07.2026) (In Russian)

7 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) // Official Journal of the European Union. 2016. L 119. P. 1–88. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed: 13.07.2026) (In English)

8 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) // Official Journal of the European Union. 2024. OJ L, 2024/1689. URL: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (accessed: 13.07.2026) (In English)

9 European Data Protection Board (2020) Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. Version 2.0. Brussels. URL: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en (accessed: 13.07.2026) (In English)

10 Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. CETS No. 223. Strasbourg, 2018. URL: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=223 (accessed: 13.07.2026) (In English)

11 Andraško J., Mesarčík M., Hamuľák O. (2021) The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework // AI & Society. Vol. 36. No. 2. P. 623–636. (In English)

12 Hacker P. (2023) A legal framework for AI training data: from first principles to the Artificial Intelligence Act // Law, Innovation and Technology. Vol. 15. No. 2. P. 257–301. (In English)

13 Wachter S., Mittelstadt B., Russell C. (2021) Why fairness cannot be automated: bridging the gap between EU non-discrimination law and AI // Computer Law & Security Review. Vol. 41. Article 105567. (In English)

14 Kaminski M.E., Malgieri G. (2021) Algorithmic impact assessments under the GDPR: producing multi-layered explanations // International Data Privacy Law. Vol. 11. No. 2. P. 125–144. (In English)

15 Smuha N.A. (2021) From a "race to AI" to a "race to AI regulation": regulatory competition for artificial intelligence // Law, Innovation and Technology. Vol. 13. No. 1. P. 57–84. (In English)

16 Veale M., Zuiderveen Borgesius F. (2021) Demystifying the Draft EU Artificial Intelligence Act: analysing the good, the bad, and the unclear elements of the proposed approach // Computer Law Review International. Vol. 22. No. 4. P. 97–112. (In English)

17 Binns R. (2022) Human judgment in algorithmic loops: individual justice and automated decision-making // Regulation & Governance. Vol. 16. No. 1. P. 197–211. (In English)

17 Adams-Prassl J., Binns R., Kelly-Lyth A. (2023) Directly discriminatory algorithms // The Modern Law Review. Vol. 86. No. 1. P. 144–175. (In English)

18 Almada M., Petit N. (2024) The EU AI Act: between product safety and fundamental rights // Common Market Law Review. Vol. 61. No. 3. P. 655–696. (In English)

19 Mantelero A. (2024) The Fundamental Rights Impact Assessment in the AI Act: roots, legal obligations and key elements for a model template // Computer Law & Security Review. Vol. 54. Article 105980. (In English)

20 Novelli C., Taddeo M., Floridi L. (2024) Accountability in artificial intelligence: what it is and how it works // AI & Society. Vol. 39. P. 1871–1882. (In English)

21 Casarosa F. (2022) Cybersecurity certification of Artificial Intelligence: a missed opportunity to coordinate between the Artificial Intelligence Act and the Cybersecurity Act // International Cybersecurity Law Review. Vol. 3. P. 5–32. (In English)

22 Peukert C., Bechtold S., Batikas M., Kretschmer T. (2022) Regulatory export and spillovers: how GDPR affects global markets for data // Management Science. Vol. 68. No. 4. P. 3186–3204. (In English)

23 Laux J., Wachter S., Mittelstadt B. (2024) Trustworthy artificial intelligence and the European Union AI Act: on the conflation of trustworthiness and acceptability of risk // Regulation & Governance. Vol. 18. No. 1. P. 3–32. (In English)

24 Judgment of the Court of Justice of the European Union of 7 December 2023, OQ v Land Hessen, Case C-634/21, ECLI:EU:C:2023:957. URL: https://curia.europa.eu/juris/liste.jsf?num=C-634/21 (accessed: 13.07.2026) (In English)

25 Judgment of the Court of Justice of the European Union of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, Case C-311/18, ECLI:EU:C:2020:559. URL: https://curia.europa.eu/juris/liste.jsf?num=C-311/18 (accessed: 13.07.2026) (In English)

26 Umitchinova B.A., Gavrilova Ju.A., Menzjuk G.A. (2025) Pravovoe regulirovanie personal'nyh dannyh v uslovijah razvitija iskusstvennogo intellekta: zarubezhnyj opyt i vyzovy dlja Kazahstana // Vestnik Instituta zakonodatel'stva i pravovoj informacii Respubliki Kazahstan. No. 3 (80). P. 37–53. DOI: 10.52026/2788-5291_2025_80_3_37 (In Russian)

27 Kusainova A.K. (2026) Problemy pravovogo regulirovanija i perspektivy sovershenstvovanija zakonodatel'stva Respubliki Kazahstan v sfere zashhity personal'nyh dannyh // Veritas Legis Journal. V. 2. No. 2. DOI: 10.62687/VLJ.2.2.2026.50 (In Russian)

ДЮСЕБАЕВ Ж.С.,*[1]
докторант.
*e-mail: z.dyussebayev@turan-edu.kz
ORCID ID: 0009-0009-5137-9835
РЕХСОН С.Н.,[1]
з.ғ.к., қауымдастырылған профессор.
e-mail: s.rekhson@turan-edu.kz
ORCID ID: 0009-0009-4710-0387
САБЕРДИНОВА А.А.,[1]
з.ғ.м., сениор-лектор.
e-mail: saberdinova@turan-edu.kz
ORCID ID: 0009-0007-5328-6443
КУДРЯВЦЕВА А.В.,[2]
з.ғ.д., профессор.
e-mail: acifna@mail.ru
ORCID ID: 0000-0001-7666-8048
[1]«Тұран» университеті,
Алматы қ., Қазақстан
[2]В.М. Лебедев атындағы
Ресей мемлекеттік әділет
университетінің
Солтүстік-Батыс филиалы,
Санкт-Петербург қ., Ресей

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНДА ЖАСАНДЫ ИНТЕЛЛЕКТІНІ ПАЙДАЛАНУ КЕЗІНДЕ ДЕРБЕС ДЕРЕКТЕРДІ ҚОРҒАУДЫҢ ИНСТИТУЦИОНАЛДЫҚ ЖӘНЕ ҚҰҚЫҚТЫҚ ТЕТІКТЕРІ: ЕУРОПАЛЫҚ МОДЕЛЬМЕН САЛЫСТЫРМАЛЫ-ҚҰҚЫҚТЫҚ ТАЛДАУ

Аңдатпа

Қазақстан Республикасында жасанды интеллектіні пайдалану кезінде дербес деректерді қорғаудың институционалдық және құқықтық тетіктері салыстырмалы-құқықтық талдауы көрсетілді. Айрықша көңіл Қазақстанның дербес деректерді қорғау туралы заңнамасы мен Еуропалық Одақтың деректерді қорғау регламенті (GDPR) және жасанды интеллект бойынша ережелері (AI Act) арасында байланыс пен айырмашылықтарды анықтауға аударылды. Зерттеудің мақсат- міндеті – инновацияны ынталандыру мен жеке өмірге кепілдік беруді ұштастыратын нормативтік негіздерді анықтау. Методолгиялық негізі ретінде формальды құқықтық, салыстырмалы-құқықтық және институционалдық тәсілдер пайдаланылды. Қазақстан Республикасының дербес деректерді қорғау, цифрландыру және жасанды интеллект саласындағы қоғамдық қатынастарды реттейтін негізгі нормативтік құқықтық актілері. Дербес деректерді, цифрлық технологияларды және жасанды интеллектіні құқықтық реттеудің өзара байланысына ерекше назар аударылды.

Тірек сөздер: жасанды интеллект, дербес деректер, цифрлық егемендік, киберқауіпсіздік, деректерді қорғау, GDPR регламенті, өңдеудің заңдылығы.

DYUSSEBAYEV Z.S.,*[1]
PhD student.
*e-mail: z.dyussebayev@turan-edu.kz
ORCID ID: 0009-0009-5137-9835
REHSON S.N.,[1]
PhD, associate professor.
e-mail: s.rekhson@turan-edu.kz
ORCID ID: 0009-0009-4710-0387
SABERDINOVA A.A.,[1]
master of law, senior lecturer.
e-mail: saberdinova@turan-edu.kz
ORCID ID: 0009-0007-5328-6443
KUDRYAVTSEVA A.V.,[2]
d.l.s., professor.
e-mail: acifna@mail.ru
ORCID ID: 0000-0001-7666-8048
[1]Turan University,
Almaty, Kazakhstan
[2]North-Western Branch of the
Lebedev Russian State University,
Saint Petersburg, Russia

INSTITUTIONAL AND LEGAL MECHANISMS FOR PERSONAL DATA PROTECTION WITHIN AI USAGE IN KAZAKHSTAN: A COMPARATIVE LEGAL ANALYSIS WITH THE EUROPEAN MODEL

Abstract

This article provides a comprehensive analysis of institutional and legal mechanisms for protecting personal data in the context of artificial intelligence (AI) usage in Kazakhstan, compared with the European regulatory framework. Special attention is given to the EU General Data Protection Regulation (GDPR) and the AI Act. The relevance of the study is justified by Kazakhstan's large-scale digital transformation and national AI strategies. The study aims to identify legal gaps and conflicts between innovation incentives in AI and privacy guarantees. Methodologically, it employs formal-legal, comparative-legal, and institutional approaches. The key regulatory acts of the Republic of Kazakhstan governing relations in the field of personal data protection, digitalization, and artificial intelligence were analyzed, along with the current strategic documents. Particular attention was paid to the interrelationship between the legal regulation of personal data, digital technologies, and artificial intelligence. It is found that Kazakhstan is actively aligning with European standards, introducing a risk-based approach to AI regulation with bans on discriminatory algorithms. However, gaps are identified: insufficient attention to prior risk assessments, limited institutional oversight, and underdeveloped rights to explanations for automated decisions. The findings are relevant for improving Kazakhstan's regulatory framework on digital sovereignty, AI, and data protection.

Keywords: artificial intelligence, personal data, digital sovereignty, cybersecurity, data protection, GDPR, lawfulness of processing.

Дата поступления статьи в редакцию: 13.07.2026