

ВЕСТНИК ИНСТИТУТА ЗАКОНОДАТЕЛЬСТВА
И ПРАВОВОЙ ИНФОРМАЦИИ
РЕСПУБЛИКИ КАЗАХСТАН
ISSN 2788-5283
eISSN 2788-5291
ТОМ 80 НОМЕР 3(2025), 37-53

УДК 34.05
ГРНТИ 10.19.61
DOI 10.52026/2788-5291_2025_80_3_37
Научная статья

© Б.А. Умитчинова^{1*}, Ю.А. Гаврилова¹, Г.А. Мензюк¹, 2025

¹ Казахстанско-Американский свободный университет, Усть-Каменогорск, Казахстан
(E-mail: ¹umitchinova.botagoz@mail.ru; ¹gavriloyuliya@yandex.kz; ¹menzjuk@mail.ru)

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В УСЛОВИЯХ РАЗВИТИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА: ЗАРУБЕЖНЫЙ ОПЫТ И ВЫЗОВЫ ДЛЯ КАЗАХСТАНА

Аннотация. Значительный прогресс технологий искусственного интеллекта расширяет возможности развития во многих сферах общественной жизни, однако, в тоже время, создает угрозы безопасности, в том числе при обработке искусственного интеллекта (далее - ИИ) персональных данных. В статье рассматриваются правовые аспекты регулирования защиты персональных данных в условиях развития искусственного интеллекта, анализируется зарубежный опыт к обеспечению конфиденциальности и оценивается текущее состояние правовой защиты персональных данных в Республике Казахстан.

Исследование основано на сравнительном правовом анализе законодательства ЕС, США, Китая и Казахстана в сфере защиты персональных данных и регулирования ИИ, анализируются различия в правоприменении и степень признания права на конфиденциальность в данных юрисдикциях. В ЕС персональные данные регулируются в рамках GDPR, который рассматривает их защиту как неотъемлемое право личности. В США подход менее унифицированный и определяется на уровне штатов, что приводит к фрагментации правового регулирования. Китай, напротив, контролирует обработку данных с позиций государственной безопасности, что ограничивает объем прав граждан на защиту их персональных данных.

В статье выявлены ключевые проблемы правоприменительной практики в Республике Казахстан, включая отсутствие конституционного признания права на защиту персональных данных, недостаточную регламентацию автоматизированного принятия решений и отсутствие механизма «права на объяснение» решений, принятых ИИ. Предлагаются меры по совершенствованию правового регулирования защиты конфиденциальности, включающих внедрение правовых норм, обеспечивающих объяснимость решений ИИ, усиление защиты персональных данных в автоматизированных системах, гармонизацию национальных норм с международными стандартами. Полученные результаты могут быть использованы для совершенствования законодательства Казахстана в сфере ИИ и персональных данных, а также для дальнейших исследований в области правового регулирования цифровых технологий.

Ключевые слова: персональные данные, искусственный интеллект, конфиденциальность, автоматизированное принятие решений, генеративный ИИ.

* Автор для корреспонденции. E-mail: umitchinova.botagoz@mail.ru.

Введение

Бурное развитие технологий искусственного интеллекта (ИИ) за последние годы предоставляет новые возможности для государств в сфере экономического, социального и культурного развития, улучшение системы здравоохранения и обороны. ИИ способен обрабатывать обширный пласт информации, который может использоваться для повышения эффективности и скорости анализа данных (в медицине – при диагностике заболеваний на основе анализа медицинских данных; финансах – для обнаружения мошенничества и алгоритмической торговли; науке и т.д.); упрощения сложных процессов принятия решений (в бизнесе, государственном секторе и др.); расширения доступности информации (переводы текстов на разные языки в реальном времени, автоматическое создание кратких выжимок из объемных отчетов); прогнозирования и предотвращения рисков (экономике, здравоохранении, моделирование последствий изменения климата и т.д.) и др.

Однако помимо положительных сторон, применение искусственного интеллекта может увеличить возможности для контроля, манипуляции и дискриминации; нарушить социальное взаимодействие; подвергнуть людей вреду в результате технологических сбоев или пренебрежения правами и социальными ценностями [1]. Кроме того, в связи с тем, что многие приложения ИИ включают в себя массовую обработку персональных данных, это затрагивает риски, касающиеся личных прав и интересов человека. Эти риски проистекают из огромного количества персональных данных, которые собирают, обрабатывают и хранят системы ИИ и могут привести к:

- утечке данных и несанкциониро-

ванному доступу к ним. Утечка данных приводит к краже личных данных, мошенничеству и другим правонарушениям. За последние пару лет произошел резкий скачок утечек персональной информации во всем мире, в сравнении с 2022 годом, в 2023 году данный показатель вырос на 111,5 % (Рисунок 1)¹;

- повторной идентификации анонимных данных. Передовые методы ИИ часто позволяют повторно идентифицировать людей, сопоставляя анонимные данные с другой доступной информацией. Этот процесс подрывает традиционные методы защиты конфиденциальности и вызывает опасения относительно эффективности текущих методов анонимизации;

- непреднамеренному использованию личной информации. Системы ИИ могут обнаруживать неожиданные корреляции или выводы из, казалось бы, безобидных данных, что может использоваться для вывода конфиденциальной информации, такой как состояние здоровья или политическая принадлежность, что потенциально приводит к дискриминации или манипуляции [2, р. 101].

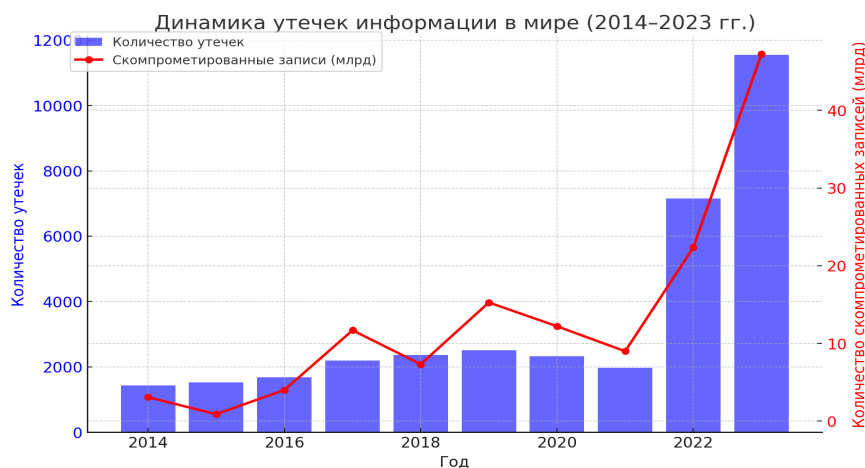


Рисунок 1. Динамика утечек персональных данных в мире (2014–2023 гг.).

В связи с этим, задача, стоящая перед исследователями и законодателем, заключается в том, чтобы найти баланс между использованием возможностей ИИ для развития общества и защитой личных прав и интересов человека,

¹ Аналитический отчет. Утечки информации в мире, 2022–2023 годы. - Экспертно-Аналитический центр InfoWatch, 2024 г. // URL: <https://www.infowatch.ru/sites/default/files/analytics/files/issledovaniye-utechek-informatsii-v-mire-za-2022-2023-gody.pdf> (дата обращения: 12.11.2024).

в том числе его персональных данных. В статье авторами на основе анализа законодательства о защите персональных данных зарубежных стран исследуются подходы и передовой зарубежный опыт достижения баланса между развитием ИИ и защитой конфиденциальности, выявляются проблемы в этой сфере в Республике Казахстан и предлагаются организационно-правовые меры по снижению рисков нарушения конфиденциальности.

Методы и материалы

В ходе исследования проблематики статьи авторами использовался метод сравнительного правового анализа, позволяющего провести анализ законодательства различных стран (ЕС, США, Китая, Казахстана) в области защиты персональных данных и их обработки системами ИИ, в ходе которого выявлены различия в подходах и правоприменительной практике. С помощью системного анализа исследованы нормативно-правовые акты, концепции и стратегии регулирования персональных данных и ИИ в различных юрисдикциях, проанализировано их влияние на баланс между развитием технологий и защитой конфиденциальности. Метод логического моделирования позволил сформулировать предложения по совершенствованию правового регулирования защиты персональных данных в Казахстане, учитывая международный опыт и текущие вызовы.

Представленные методы дали возможность комплексно исследовать проблему, выявить правовые риски, оценить международный опыт и предложить меры по совершенствованию регулирования защиты персональных данных в Республике Казахстан.

Результаты и обсуждение

В цифровую эпоху определение правового статуса персональных данных имеет большое значение для их защиты. Различные государства придерживаются собственных подходов

к установлению правовой природы данного понятия. В ЕС статья 4 GDPR определяет персональные данные как любую информацию, относящуюся к человеку, которая идентифицирует или может идентифицировать человека. В GDPR право субъекта данных на его персональные данные характеризуется как «право на неприкосновенность частной жизни в отношении обработки персональных данных»². Такое право считается основным и не может быть перевешено другими ценностями. Кроме того, статья 16 Договора о функционировании Европейского союза обязывает ЕС устанавливать правила, касающиеся защиты лиц в отношении обработки персональных данных³.

В США право на защиту персональных данных более узко трактуется как «право быть в одиночестве» (right to be left alone) и является частью гражданских свобод, закрепленных Конституцией США. Защита данных обеспечивается фрагментарно на уровне штатов (например, закон CCPA в Калифорнии), что дает меньше единообразия в правовом регулировании, чем в ЕС.

В китайском законодательстве определение персональных данных закреплено в Законе Китая о кибербезопасности. Согласно статье 67(5) Закона, персональные данные охватывают различные сведения, к которым относятся, в частности, имя, дата рождения, персональный идентификационный номер, биометрические характеристики, место проживания и контактный телефон [3]. В КНР защита персональных данных не рассматривается как неотъемлемое право, в отличие от права на частную жизнь или собственности, и уровень ее охраны остается сравнительно низким. Это связано с несколькими факторами. Во-первых, в отличие от ЕС, китайское законодательство не признает персональные данные основополагающим правом человека. Власти Китая, как крупнейший оператор данных, считают, что право граждан на защиту своей информации должно быть ограничено, если оно мешает государству собирать, обрабатывать, хранить

² General Data Protection Regulation (GDPR), adopted on April 27, 2016, and enforced since May 25, 2018 // URL: <https://gdpr-info.eu/> (date of reference: 15.11.2024).

³ Treaty on the Functioning of the European Union of 13 December 2007 - consolidated version // URL: https://eur-lex.europa.eu/eli/treaty/tfeu_2012/oj/eng (date of reference: 15.11.2024).

и использовать эти данные. Во-вторых, Конституция Китая предоставляет минимальные гарантии защиты личной информации, включая лишь место жительства, свободу и тайну переписки. Однако персональные данные охватывают гораздо более широкий спектр информации, который выходит за рамки этих конституционных положений [3].

В Республике Казахстан правовой режим защиты персональных данных, по мнению авторов, близок к китайскому подходу, поскольку в Основном законе государства защита персональных данных не отражена как конституционное право человека, в ст. 18 закреплены лишь права на неприкосновенность частной жизни, личную и семейную тайну, тайну личных вкладов и сбережений, переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений⁴.

Таким образом, правовая природа персональных данных определяет режим защиты этих данных в различных государствах. Разные подходы государств к их определению и защите устанавливают границы возможностей использования данных и степень их конфиденциальности, особенно в эпоху развития искусственного интеллекта и цифровых технологий, в связи с тем, что персональные данные становятся «цифровым ресурсом». Поэтому необходим анализ правовых актов и нормативных рамок использования персональных данных в ИИ в зарубежных странах для выявления проблем защиты этих данных и возможности адаптации успешных международных практик в Республике Казахстан.

Европейский союз стал мировым лидером по защите персональной информации. Принятие Общего регламента ЕС по защите данных (GDPR) (вступил в силу 24 мая 2016 года и применяется с 25 мая 2018 года) стало важным шагом на пути к укреплению права человека на защиту персональных данных в цифровую эпоху и упрощению ведения бизнеса путем уточнения правил для компаний и государственных органов на цифровом

рынке. Единый закон значительно снижает фрагментацию в различных национальных системах и убирает ненужное административное бремя⁵. Регламент применяется в любой организации, которая обрабатывает персональные данные граждан ЕС, независимо от места нахождения организации. В GDPR применяются некоторые термины, относящиеся к интернету (Интернет, социальные сети, веб-сайт, ссылки и т. д.), но не содержатся понятия, относящиеся к искусственному интеллекту. Это свидетельствует о том, что Регламент направлен на урегулирование проблем конфиденциальности, связанных с использованием интернета, которые не были охвачены Директивой о защите данных 1995 года, но стали актуальными к моменту разработки GDPR, однако вопросы, касающиеся ИИ, которые приобрели социальную значимость только в последние годы, не рассмотрены.

GDPR построен на нескольких ключевых принципах защиты персональных данных, однако их внедрение сталкивается с трудностями из-за быстро развивающихся технологий, включая ИИ:

- принцип законности, справедливости и прозрачности (статья 5(1)(a)) сталкивается с трудностями в применении из-за сложности алгоритмов ИИ, что затрудняет их восприятие пользователями. В соответствии с GDPR, для соблюдения данного принципа субъектам данных необходимо предоставлять ясную и полную информацию о причинах, значении и возможных последствиях обработки их данных (Преамбула 71) [4];

- принцип ограничения цели (статья 5(1)(b)) требует, чтобы сбор данных осуществлялся для «определенных, явных и законных целей» без дальнейшей обработки в несовместимых целях. В то же время, алгоритмы машинного обучения часто требуют больших объемов данных, а цели их использования могут быть плохо определены, что нарушает этот принцип [4];

- принцип минимизации данных (статья 5(1)(c)) требует сбора только не-

⁴ Конституция Республики Казахстан от 30 августа 1995 года // URL: https://adilet.zan.kz/rus/docs/K950001000_/links (дата обращения: 21.11.2024).

⁵ European Commission. "Data protection in the EU." European Commission - European Commission, 30 April 2021 // URL: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en (date of reference: 25.11.2024).

обходимых данных, однако ИИ-системы могут анализировать новые категории данных, выходя за рамки первоначального сбора. Например, алгоритм может выявить сексуальную ориентацию или политические взгляды человека по активности в соцсетях, что противоречит принципу минимизации [5];

- принцип ответственности (статья 5(2)) обязывает контролера данных не только соблюдать GDPR, но и доказывать его выполнение. Это требует четких политик и процедур, подтверждающих соблюдение регламента. GDPR также предусматривает право на объяснение решений ИИ, однако степень его детализации остаётся спорной. ЕС акцентирует внимание на объяснимости ИИ, поскольку это необходимо для соблюдения принципов точности и подотчетности. Суды могут требовать объяснений алгоритмических решений, чтобы обеспечить защиту прав пострадавших [4]. Без этого невозможно обеспечить человеческий контроль над ИИ, а также дать пострадавшим возможность эффективно защищать свои права и добиваться возмещения ущерба⁶.

Таким образом, несмотря на то что Регламент предлагает прочную основу для защиты персональных данных, такие особенности ИИ, как его сложность, непрозрачность и высокая потребность в данных, создают определенные проблемы для соблюдения принципов и механизмов GDPR. Важно отметить, что GDPR применяется не только к традиционной обработке данных, но и к более современным технологиям. Во-первых, хотя сам термин «искусственный интеллект» не упоминается в тексте Регламента, в нем есть несколько положений, касающихся ИИ-систем. Например, статья 22 защищает людей от решений, которые принимаются полностью автоматически, без участия человека (автоматизированное принятие решений (ADM)). Согласно этому положению, каждый человек имеет право не подвергаться ADM, если оно может негативно повлиять на его права, юридический статус или другие важные аспекты жизни [6, p. 11]. Во-вторых, положения GDPR применяются

к многим ИИ-системам, поскольку Регламент включает механизмы для защиты данных в процессе их обработки.

Закон ЕС об искусственном интеллекте, принятый в 2024 году, регулирует использование систем ИИ на основе рисков, уделяя особое внимание угрозам конфиденциальности и защите данных. Это подчеркивает тесную связь между GDPR и Законом ЕС об ИИ. GDPR, как технологически нейтральный акт, применяется к системам ИИ в случае обработки персональных данных на любом этапе их жизненного цикла. Большинство требований Закона об ИИ распространяются на системы высокого риска (перечислены в статье 6 и Приложении III). Организации, работающие с ИИ и персональными данными, обязаны соблюдать нормы обоих актов [7].

GDPR и Закон об ИИ отражают стремление ЕС к комплексному управлению конфиденциальностью данных в эпоху ИИ. Человекоцентричный и этический подход ЕС обеспечивает защиту прав и конфиденциальности, однако строгие стандарты могут замедлить темпы разработки и внедрения ИИ по сравнению с регионами с менее жестким регулированием [8].

В США, напротив, нормативные рамки для ИИ менее предписывающие и создающие основу к более быстрому развитию ИИ и инноваций, хотя и с меньшим акцентом на конфиденциальность и этические гарантии. К тому же, в отличие от европейского подхода к защите персональных данных, сделавшего акцент на централизованное регулирование (GDPR), подход США децентрализованный и основан на сочетании федеральных и отраслевых норм. Как ЕС, США сталкиваются с необходимостью адаптироваться к новым вызовам, связанным с ИИ, однако стратегии государств к решению этих проблем различны. Подход к регулированию ИИ в США преимущественно реактивный и отраслевой, при этом нет единого федерального закона, охватывающего весь спектр технологий ИИ и их

⁶ Ai, Data Governance and Privacy Synergies and Areas of International Co-operation. OECD Artificial Intelligence Papers, June 2024 No. 22, 55 p. // URL: https://ai.radensa.ru/wp-content/uploads/2024/07/AI_data_governance_and_privacy_Synergies_and_areas_of_international.pdf (date of reference: 02.12.2024).

последствий [9, p. 53].

Фрагментированный подход к регулированию рассматриваемых отношений отражает историческое развитие законов о конфиденциальности в США, где законодательство развивалось в ответ на конкретные проблемы, а не как часть скоординированной национальной стратегии. Например, Закон о переносимости и подотчетности медицинского страхования (HIPAA) регулирует безопасность персональных данных в секторе здравоохранения, обеспечивая конфиденциальность медицинской информации; Закон Грэмма-Лича-Блайли (GLBA) устанавливает стандарты защиты финансовой информации [10, p. 1368], также были приняты Закон о правах и конфиденциальности в сфере образования семьи (FERPA), Закон о защите конфиденциальности детей в Интернете (COPPA), Закон о защите конфиденциальности видео (VPPA) и др. [6, p. 12]. Отсутствие всеобъемлющего федерального регулирования защиты персональных данных, привело к принятию законодательных актов на уровне штатов. Такие законы, как Закон Калифорнии о конфиденциальности потребителей (CCPA) 2018 г., Закон о конфиденциальности Нью-Йорка (NYPA), 2021 г., Закон о конфиденциальности Колорадо (CPA) 2021 г., Закон о защите данных потребителей Вирджинии (VCDPA) 2023 г. и другие создают сложную и непоследовательную нормативную среду по всей стране.

Закон Калифорнии о конфиденциальности потребителей (CCPA), принятый в 2018 году, является одним из самых важных законов о конфиденциальности на уровне штатов в Соединенных Штатах, существенно влияющих на ландшафт ИИ. Первоначально созданный для защиты конфиденциальности жителей Калифорнии, этот закон стал важным правовым документом для регулирования использования данных ИИ [11]. CCPA предоставляет жителям Калифорнии права в отношении их персональных данных, включая право

на доступ, удаление и отказ от продажи своих данных. Эти права имеют решающее значение в контексте ИИ, где большие объемы персональных данных часто используются для обучения алгоритмов и повышения производительности системы⁷.

Соответственно, положения CCPA напрямую влияют на системы ИИ несколькими способами:

- доступ к данным и удаление. Разработчики и компании ИИ должны выполнять запросы потребителей на доступ к их данным или их удаление;
- отказ от продажи данных. Закон позволяет потребителям отказаться от продажи своих персональных данных;
- прозрачность и подотчетность. Компании должны раскрывать свои методы сбора и обработки данных, что может повысить подотчетность и укрепить доверие к приложениям ИИ [12].

Таким образом, фрагментация законодательства о защите данных в США создает значительные проблемы из-за отсутствия единого федерального регулирования. Это приводит к разрозненности требований в разных штатах, что влечет за собой несколько сложностей:

- компании, работающие в нескольких штатах, сталкиваются с увеличением расходов и операционной сложности из-за необходимости соблюдать разные законы [13];
- отсутствие единообразия вызывает непоследовательную защиту конфиденциальности для потребителей в зависимости от их штата проживания, что подрывает эффективность мер защиты данных;
- постоянные изменения в нормативной среде на уровне штатов создают неопределенность для бизнеса, затрудняя адаптацию к новым требованиям;
- соблюдение множества различных законов усложняет инновации, особенно для стартапов и малых компаний, которым сложно ориентироваться в разрозненных правилах [10, p. 1371].

Принятый на федеральном уровне Закон о национальной инициативе в области искусственного интеллекта (2021 г.) ориентирован на поддержку научных исследований и разработок

⁷ California Consumer Privacy Act (CCPA), enacted on June 28, 2018, and effective since January 1, 2020 // URL: <https://oag.ca.gov/privacy/ccpa> (date of reference: 10.12.2024).

в области ИИ, а не на установление нормативных ограничений его применения. Этот законодательный акт направлен на стимулирование инноваций, однако не включает всесторонние меры, специально разработанные для устранения рисков, связанных с конфиденциальностью данных в технологиях ИИ [14, p. 1248].

Исходя из вышеизложенного, сегментированный нормативный ландшафт и отсутствие единой федеральной структуры создают значительные проблемы в защите конфиденциальности персональных данных в контексте ИИ в США. Фрагментированный характер нормативных актов США означает, что защита конфиденциальности может быть непоследовательной и менее комплексной по сравнению с более унифицированным и предупредительным подходом ЕС. Решение этих проблем потребует принятия федерального законодательства о конфиденциальности, аналогичного GDPR, являющимся необходимым предварительным условием для любого регулирования, которое явно нацелено на системы ИИ [15]. В то же время, ориентированный на инновации регулирующий подход США имеет тенденцию отдавать приоритет быстрой разработке и рыночным решениям. Отсутствие всеобъемлющего федерального регулирования ИИ обеспечивает большую гибкость и более быстрое внедрение новых технологий.

Режим защиты персональных данных в Китае демонстрирует существенные различия по сравнению с режимами ЕС и США. В отличие от GDPR, который характеризуется широкой сферой охвата, всеобъемлющим установлением стандартов и обеспечением их соблюдения, законодательство Китая в этой сфере не является унифицированным - действующие нормативные акты нацелены только на регулирование ряда конкретных секторов. Эти целевые законы включают общие требования, а установление стандартов и обеспечение их соблюдения осуществляется рядом регулирующих органов, наиболее значимыми из которых являются соответствующие министерства Государственного совета. В отличие от отраслевых законов в

США, которые больше ориентированы на государственный сектор, китайские законы предоставляют гражданам некоторую базовую защиту от частных сетевых операторов, но оставляют обработку персональных данных в государственном секторе в значительной степени нерегулируемой [16]. Еще одним фундаментальным различием между подходом КНР и подходами ЕС и США заключается в том, что последние отстаивают индивидуальную конфиденциальность как главный интерес, в то время как китайский подход предпочитает отдавать приоритет общественной безопасности [16].

Длительное время недостаточно развитая цифровая индустрия Китая обуславливала непоследовательное регулирование конфиденциальности и защиты данных. Однако цифровая трансформация экономики и связанные с этим проблемы - утечка данных, ценовая дискриминация и недобросовестная конкуренция среди интернет-компаний - заставили Китай усилить киберуправление. Рост глобальной конкуренции и угроз кибербезопасности также способствовал ужесточению законодательства о защите данных с 2010-х годов [17].

10 ноября 2021 года Китай принял Закон о защите персональной информации (PIPL), направленный на предотвращение злоупотреблений личными данными частными компаниями и государственными органами. Подобно GDPR (ЕС) и CCPA (США), закон запрещает автоматизированное принятие решений и требует получения согласия субъектов на обработку данных [6, p. 13]. Однако в судебной практике Китая права на персональные данные пока не признаны отдельным гражданским правом. Отсутствие четкой классификации прав на персональную информацию заставляет граждан обращаться за защитой через смежные права, такие как право на неприкосновенность частной жизни. Это затрудняет эффективное возмещение ущерба и приводит к консервативному подходу судов в подобных делах, создавая правовую неопределенность [18].

В июле 2023 года Китай принял первый регламент по

генеративному ИИ — «Временные меры по администрированию услуг генеративного искусственного интеллекта» (Меры по ИИ), разработанные Администрацией киберпространства Китая (CAC) совместно с другими ведомствами [17]. Меры направлены на обеспечение безопасности генеративного ИИ, включая защиту конфиденциальности и персональных данных, в соответствии с PIPL, Законом о кибербезопасности (CSL) и Законом о безопасности данных (DSL). Меры представляют собой руководящие принципы, а не детальные правила, поскольку законодатели Китая не имели полного понимания технологий генеративного ИИ. Они интегрируют существующие законы, создавая правовую основу для регулирования ИИ без установления конкретных норм по обработке данных и обязанностям провайдеров [17].

Исследование законодательства и научных трудов выявляет особенности правового режима защиты персональных данных в КНР. Во-первых, несмотря на создание правовой основы для защиты данных, нормы отстают от требований, предъявляемых генеративным ИИ в публичном и частном праве. Во-вторых, китайское законодательство рассматривает сетевую безопасность как ключевой элемент национальной безопасности, что подтверждается Законом о национальной безопасности Китая, устанавливающим принцип «осознанного согласия» для трансграничной передачи данных [19]. В-третьих, в Китае отсутствует единый надзорный орган по защите данных - контроль распределен между различными министерствами, что затрудняет соблюдение законодательства по сравнению с ЕС, где действует единый регулирующий орган.

Республика Казахстан (далее - РК) находится на начальном этапе развития правового регулирования ИИ и защиты персональных данных в контексте применения искусственного интеллекта. В отличие от ЕС, ставящего во главу угла права граждан и прозрачность алгоритмов; США, делающих упор на инновации; КНР, интегрировавшей защиту данных в

национальную стратегию безопасности и характеризующейся высоким уровнем государственного контроля, Казахстану предстоит определить свой путь.

В РК правовую основу законодательства о персональных данных составляет Закон РК «О персональных данных и их защите» от 21 мая 2013 года, приказ Министра цифрового развития, инноваций и аэрокосмической промышленности РК «Об утверждении Правил осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных» от 12 июня 2023 года, Закон РК «Об информатизации» от 24 ноября 2015 года, постановление Правительства РК «Об утверждении Концепции кибербезопасности («Киберщит Казахстана») от 30 июня 2017 года, Постановление Правительства РК «Об утверждении Концепции развития искусственного интеллекта на 2024 – 2029 годы» от 24 июля 2024 года и др.

Закон РК «О персональных данных и их защите» регулирует общественные отношения, связанные со сбором, обработкой, хранением и защитой персональных данных. Данный нормативный акт является важным инструментом регулирования использования и защиты персональных данных, однако, в связи с развитием технологий, особенно искусственного интеллекта, требуется его адаптация для учета новых вызовов, таких как автоматизированная обработка данных и необходимость разъяснения решений, принимаемых ИИ. Благодаря использованию искусственного интеллекта персональные данные становятся не просто объектом защиты, а ценным ресурсом, который активно применяется для анализа, прогнозов и воздействия на поведение человека [20].

Вместе с тем, в условиях стремительной цифровизации существенно возрастает угроза утечки и неконтролируемого использования, что усиливает потребность в эффективных механизмах правовой защиты. Учитывая данные обстоятельства, в Концепции развития искусственного интеллекта на 2024 – 2029 годы одним из принципов внедрения искусственного интеллекта

является конфиденциальность, акцентирующий внимание на необходимости обеспечить защиту персональных данных, частной жизни человека и других охраняемых законом тайн⁸.

Как и Общий регламент ЕС по защите данных (GDPR) Закон РК устанавливает базовые принципы обработки персональных данных, однако между ними есть концептуальные различия в детализации, масштабе регулирования и правах субъектов данных. Принципы, закрепленные в нормативном акте РК, носят более общий характер (соблюдение конституционных прав и свобод человека и гражданина, законность, конфиденциальность персональных данных ограниченного доступа, равенство прав субъектов, собственников и операторов, обеспечение безопасности личности, общества и государства)⁹, тогда как принципы GDPR ЕС имеют отраслевой характер (ограничение целью, минимизация данных, достоверность персональных данных, ограничение срока хранения персональных данных, целостность и конфиденциальность)¹⁰, позволяющий более жестко регламентировать порядок обработки персональных данных. К тому же, казахстанский Закон имеет меньше детализированных требований по обработке данных, GDPR более строгий в отношении прозрачности, минимизации данных и сроков их хранения.

В то же время, в законодательстве о персональных данных правовой статус искусственного интеллекта не определен, однако существует разделение между обработкой данных с использованием средств автоматизации и без использования таковых. В Закон РК «Об информатизации» введена ст. 18-1. Права и обязанности собственника и владельца интеллектуального робота, п. 2 которой возлагает обязанность на собственников и владельцев интеллектуального робота

информировать субъекта персональных данных об автоматизированной обработке¹¹. В свою очередь, пп. 43-1 ст. 1 вышеуказанного Закона определяет интеллектуального робота как автоматизированное устройство, совершающее определенное действие или бездействующее с учетом воспринятой и распознанной внешней среды. По мнению Тлембаевой Ж.У., отсутствие в законодательстве четкого определения понятия «искусственный интеллект» обусловлено тем, что оно во многом пересекается и частично сливается по смыслу с термином «искусственный (интеллектуальный) робот» [21, с. 65].

В соответствии с мировыми стандартами защиты персональных данных, в ст. 36 Закона РК «Об информатизации» были внесены дополнения, направленные на ограничение автоматизированного принятия решений, а также на повышение прозрачности обработки персональных данных. Они оказывают значительное влияние на защиту персональной информации в условиях развития искусственного интеллекта. Закон запрещает принимать решения на основании исключительно автоматизированной обработки данных, если такие решения влияют на права и законные интересы граждан. Данный запрет предотвращает дискриминационные или несправедливые решения, принимаемые без участия человека. Также владельцы и собственники электронных информационных ресурсов обязаны уведомлять субъектов персональных данных, если их информация обрабатывается автоматически и это влияет на их права, что повышает прозрачность обработки персональных данных.

Таким образом, минимизация рисков использования персональных данных субъектов искусственным интеллектом достигается с помощью того, что Закон:

⁸ Постановление Правительства Республики Казахстан от 24 июля 2024 года № 592 «Об утверждении Концепции развития искусственного интеллекта на 2024 – 2029 годы» // URL: <https://adilet.zan.kz/rus/docs/P2400000592> (дата обращения: 15.12.2024).

⁹ Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» // URL: <https://adilet.zan.kz/rus/docs/Z1300000094/z13094.htm> (дата обращения: 15.12.2024).

¹⁰ General Data Protection Regulation (GDPR), adopted on April 27, 2016, and enforced since May 25, 2018 // URL: <https://gdpr-info.eu/> (дата обращения: 15.12.2024).

¹¹ Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации» // URL: <https://adilet.zan.kz/rus/docs/Z1500000418> (дата обращения: 15.12.2024).

- обязывает информировать субъект о том, как его данные используются;
- позволяет субъекту влиять на процесс принятия решений и требовать объяснений;
- запрещает полностью автоматизированные решения без согласия человека.

Однако, несмотря на позитивные стороны, есть ряд нерешенных вопросов. Во-первых, Закон не содержит механизма объяснения решений ИИ, тогда как в ЕС (GDPR) закреплено «право на объяснение», которое дает гражданину возможность узнать, как алгоритм пришел к решению. Во-вторых, в законодательстве не определен механизм контроля выполнения запрета (например, в банках или государственных структурах может использоваться скрытая автоматизация). В-третьих, не определены штрафы или санкции за нарушение данных норм.

Статья 56 Закона РК «Об информатизации» обязывает собственников и операторов информационных систем защищать персональные данные с момента их получения до уничтожения или обезличивания. В условиях развития ИИ это положение приобретает особую значимость, поскольку алгоритмы машинного обучения широко используют персональные данные для анализа и принятия решений. Закон возлагает обязанность по защите персональных данных не только на операторов, но и на третьи лица, которые могут передавать или обрабатывать данные. Это ключевой момент в регулировании ИИ, так как алгоритмы часто используют большие массивы информации, передаваемой различными компаниями и государственными органами. Важно, что Закон закрепляет защиту данных с момента их получения до уничтожения на всех этапах их использования - сбор данных, обучение алгоритмов, хранение, передача третьим лицам, удаление данных. Принцип «защиты на всем жизненном цикле данных» присутствует и в GDPR, где также предусмотрено обязательство защиты данных на всех стадиях их обработки, однако в Казахстане опять же не определены четкие механизмы контроля за соблюдением этих норм.

Одним из ключевых вопросов, на сегодняшний день, является консолидация законодательства в сфере защиты персональных данных. Закон РК «О персональных данных и их защите», принятый в 2013 году, во многом устарел и не учитывает современные цифровые реалии. В этой связи актуальной представляется разработка нового комплексного закона о персональных данных, который бы интегрировал положения действующего законодательства, включая нормы Закона РК «Об информатизации», касающиеся защиты данных в условиях использования ИИ и интеллектуальных систем. Таким образом, для усиления защиты персональных данных в эпоху ИИ Казахстану важно разработать специализированное законодательство и ориентироваться на лучшие мировые практики, учитывая национальные особенности. На данный момент в Республике Казахстан разработана национальная стратегия ИИ и на стадии завершения законопроект об ИИ, который должен обеспечить баланс между стимулированием развития и регулированием сферы ИИ, в том числе при использовании персональных данных при машинном обучении и автоматизированной обработке.

Заключение

Персональные данные в цифровую эпоху приобретают двойственную природу: с одной стороны, они являются объектом правовой защиты, с другой - ценным цифровым ресурсом, используемым в системах искусственного интеллекта для анализа, прогнозирования и принятия решений, что требует усиления правового режима их охраны. ИИ значительно увеличивает риски нарушения конфиденциальности, включая возможность утечки данных, повторной идентификации анонимной информации и принятия автоматизированных решений без участия человека. При этом нарушаются фундаментальные права личности, в том числе на неприкосновенность частной жизни и справедливое обращение.

Анализ международного опыта правового регулирования персональных данных в мире показывает, что разные страны по-разному трактуют

правовую природу персональных данных, что влияет на степень их защиты. В Республике Казахстан право на защиту персональных данных не признана конституционным, что делает его регулирование менее жестким и зависимым от текущей государственной политики. Этот вопрос остается предметом дискуссий. Среди государств СНГ Республика Узбекистан в статье 31 Конституции закрепила право каждого на защиту персональных данных, включая возможность требовать исправления недостоверной информации, а также удаления данных, собранных незаконным путем или утративших правовые основания.

На сегодняшний день законодательные нормы Республики Казахстан в области защиты персональных данных развиваются в соответствии с глобальными тенденциями. Вместе с тем, в сравнении с правовыми системами Европейского союза, США и Китая, казахстанское регулирование демонстрирует ряд существенных пробелов, особенно в контексте цифровой трансформации и развития технологий искусственного интеллекта. В частности, в законодательстве отсутствует достаточная детализация таких ключевых принципов, как минимизация сбора данных, ограничение сроков хранения, прозрачность обработки, а также целевая обусловленность и точность персональных данных, что приводит к высоким рискам злоупотреблений и нарушения прав субъектов данных.

В отличие от Общего регламента по защите данных Европейского союза (GDPR), в казахстанской правовой системе не предусмотрены:

- специализированные механизмы контроля за соблюдением указанных принципов;

- институционализируемая ответственность за нарушение стандартов защиты;

- четко сформулированное «право на объяснение» алгоритмических решений, обеспечивающее субъектам данных возможность понимать логику, последствия и правовые основания решений, принятых ИИ.

Хотя в Законе Республики Казахстан

«Об информатизации» закреплены положения, ограничивающие автоматизированное принятие решений, это следует рассматривать лишь как начальный этап регулирования. Современные условия требуют более продвинутого и комплексного подхода. В целях модернизации законодательства предлагается:

- инкорпорировать принципы GDPR в казахстанскую правовую систему, при этом адаптируя их к национальному контексту и техническим реалиям;

- уточнить правовые принципы обработки персональных данных, сделав их более специализированными, в том числе в части минимизации объема обрабатываемых данных, ограничения целей и сроков хранения, установления обязанностей по обеспечению прозрачности и отчетности;

- закрепить на законодательном уровне «право на объяснение» автоматизированных решений. Предлагается дополнить статью 22 проекта Закона РК «Об искусственном интеллекте» пунктом 4 «Субъекты персональных данных имеют право на получение понятного и обоснованного объяснения логики, значимости и предполагаемых последствий решений, принятых системой искусственного интеллекта без участия человека, если такие решения затрагивают их права и законные интересы»;

- разработать механизмы апелляции решений, принятых ИИ, а также процедурные гарантии участия человека при вынесении социально значимых решений.

Действующее национальное законодательство в сфере защиты персональных данных фрагментировано - регулирование разбросано по различным нормативным актам (Закон «О персональных данных и их защите», Закон «Об информатизации» и др.), что создает правовую неопределенность, особенно в условиях развития ИИ. В связи с этим, Казахстану требуется разработка единого закона о персональных данных, включающий положения об их обработке в системах ИИ.

Таким образом, для Казахстана важно разработать сбалансированную модель регулирования персональных данных, которая гармонизирует

защиту персональных данных с способствующих замедлению международными стандартами, инноваций, и создает четкие правила стимулирует развитие ИИ, взаимодействия государства, бизнеса и избегая чрезмерных ограничений, граждан в сфере обработки данных.

Вклад авторов

Автор **Умитчинова Б.А.** - внесла существенный вклад в разработку концепции и содержания статьи. Автором был проведен анализ научной литературы и нормативных материалов по теме исследования и предложены основные выводы.

Автор **Гаврилова Ю.А.** - разработала методологическую основу исследования, обосновав теоретические аспекты рассматриваемой темы. Кроме того, автор участвовала в редактировании текста, обеспечивая логическую последовательность изложения и соответствие статьи научным требованиям.

Автор **Мензюк Г.А.** - провела критический пересмотр содержания работы, утвердила окончательный вариант статьи для публикации, осуществила надлежащее изучение и решение вопросов, связанных с достоверностью данных и целостностью всех частей статьи.

Список литературы:

1. Sartor, G. The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. Study Panel for the Future of Science and Technology. EPRS European Parliamentary Research Service // G.Sartor // - Brussels, European Union, 2020. - 84 p. // Retrieved from [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf) (date of reference: 15.11.2024).

2. Rajesh, V. Navigating the Privacy Paradox: Balancing AI Advancement and Data Protection in the Digital Age // V.Rajesh, K.Adapa // International Journal of Scientific Research in Computer Science, Engineering and Information Technology. - No10(6). - P. 99-110.

3. Huang, J. Applicable Law to Transnational Personal Data: Trends and Dynamics // J. Huang // German Law Journal. - 2020. - Volume 21. - Issue 6. - P. 1283-1308. // Retrieved from <https://www.cambridge.org/core/journals/german-law-journal/article/applicable-law-to-transnational-personal-data-trends-and-dynamics/28B05974FD63C50F-8BA6EA079B66C6B5> (date of reference: 21.11.2024).

4. Pierre, L. Data Protection in AI-Driven Systems: Understanding the EU's Legal and Regulatory Response Through the General Data Protection Regulation (GDPR) // L. Pierre, U.Barrat // IE University Law School. - June 12th, 2023. // Retrieved from https://www.researchgate.net/publication/385089185_Data_Protection_in_AI-Driven_Systems_Understanding_the_EU's_Legal_and_Regulatory_Response_Through_the_General_Data_Protection_Regulation_GDPR (date of reference: 25.11.2024).

5. Wachter, S. "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation" // S.Wachter, B.Mittelstadt, L.Floridi // International Data Privacy Law. - 2017. - Volume 7. - No2. // Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469 (date of reference: 27.11.2024).

6. King, J. Rethinking Privacy in the AI Era Policy Provocations for a Data-Centric World. // J. King, C.Meinhardt // - Stanford University. White Paper. - February 2024. - 53 p.

7. Clark, J. Europe: The EU AI Act's relationship with data protection law: key take-aways. // J.Clark, M.Demircan, K.Kettas // Retrieved from <https://privacymatters.dlapipiper.com/2024/04/europe-the-eu-ai-acts-relationship-with-data-protection-law-key-take-aways/> (date of reference: 06.12.2024).

8. Mittelstadt, B. AI ethics—too principled to fail? // B. Mittelstadt // Journal of Ethics and Information Technology. - 2019. - No21(4). - P. 345-358 // Retrieved from https://www.researchgate.net/publication/333874695_AI_Ethics_-_Too_Principled_to_Fail (date of reference: 10.12.2024).

9. Binns, R. The lack of comprehensive AI regulation in the US: An overview. //

R. Binns // Journal of Technology Law & Policy. - 2022. - No23(1). - P. 45-67.

10. Atata, B. The AI Privacy Paradox: a Comparative Analysis of EU and US Approaches to Regulating Artificial Intelligence and Protecting Personal Data // B.Atata // International Research Journal of Modernization in Engineering Technology and Science. - 2024. - Volume 6. - Issue 9. - P. 1363-1377.

11. Ijaiya, H., Adeniyi, I. AI and Personal Data Privacy in the U.S: Balancing Customer Convenience with Privacy Compliance // H.Ijaiya, I.Adeniyi // ABUAD Law Journal (ALJ). – 2024. Vol. 12. - Issue 1. - P. 41-64. // Retrieved from <https://doi.org/10.53982/alj.2024.1201.03-j> (date of reference: 25.12.2024).

12. Kang, C. How state privacy laws are reshaping the tech landscape // C. Kang // The New York Times. - 2021. // Retrieved from <https://nytimes.com> (date of reference: 30.12.2024).

13. Greenleaf, G. Global data privacy laws 2023: The emerging landscape. Privacy Law & Policy Report. - 2023. // G.Greenleaf // Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4426146 (date of reference: 05.01.2025).

14. Smith, B. The state of AI regulation: Challenges and opportunities // B. Smith // Harvard Law Review. - 2022. - No135(4). - P. 1234-1260.

15. Ratnam, G. Data privacy law seen as needed precursor to AI regulation. // G. Ratnam // Retrieved from <https://rollcall.com/2023/09/26/data-privacy-law-seen-as-needed-precursor-to-ai-regulation/> (date of reference: 10.01.2025).

16. Feng, Y. Personal Data Protection at the Crossroad in China: Legal Framework, Practical Problems and Suggested Reforms // Y.Feng // Asia Pacific Law Review. - 2019. - No27:1. - P. 62-82. // Retrieved from https://www.researchgate.net/publication/334995413_The_future_of_China's_personal_data_protection_law_challenges_and_prospects (date of reference: 13.01.2025).

17. Xiongbiao, Y. Privacy and personal data risk governance for generative artificial intelligence: A Chinese perspective // Y. Xiongbiao, Y. Yuhong, J.Li, B.Jiang // Telecommunications Policy. - 2024. - No48. // Retrieved from <https://doi.org/10.1016/j.tel-pol.2024.102851> (date of reference: 16.01.2025).

18. Chen, Z., et al. Securing privacy in the digital age: The quest for judicial protection of personal information // Z.Chen, R.Geng, Z.Jia, et al. // Journal of Infrastructure, Policy and Development. - 2024. - No8(12). // Retrieved from <https://doi.org/10.24294/jipd.v8i12.9253> (date of reference: 20.01.2025).

19. Yang, L. Practice and Prospect of Regulating Personal Data Protection in China // L.Yang, Y.Lin, B. Chen // Laws. - 2024. - No13. // Retrieved from <https://doi.org/10.3390/laws13060078> (date of reference: 20.01.2025).

20. Гусарова, А. Защита персональных данных в Казахстане 2.0: цифровой след COVID-19. Проект при финансовой поддержке Фонда Сорос-Казахстан // А. Гусарова, С. Джаксылыков // - 2021. // [Электронный ресурс]. – Режим доступа: https://www.soros.kz/wp-content/uploads/2021/03/Personal-Data_Covid-Implications.pdf (дата обращения: 20.03.2025).

21. Тлембаева, Ж.У. О некоторых подходах к правовому регулированию искусственного интеллекта // Ж.У. Тлембаева // Вестник Института законодательства и правовой информации Республики Казахстан. - 2021. - №2(65). - С. 61-74.

© Б.А. Умитчинова¹, Ю.А. Гаврилова¹, Г.А. Мензюк¹, 2025

¹ Қазақстан-Американдық еркін университеті, Өскемен, Қазақстан
(E-mail: ¹umitchinova.botagoz@mail.ru; ¹gavriloyuliya@yandex.kz; ¹menzjuk@mail.ru)

ЖАСАНДЫ ИНТЕЛЛЕКТІ ДАМУ ЖАҒДАЙЫНДАҒЫ ЖЕКЕ ДЕРЕКТЕРДІ ҚҰҚЫҚТЫҚ РЕТТЕУ: ШЕТЕЛДІК ТӘЖІРИБЕ ЖӘНЕ ҚАЗАҚСТАН ҮШІН ТӨНЕТІН ҚАТЕРЛЕР

Аннотация. Жасанды интеллект технологияларының айтарлықтай ілгерілеуі қоғамдық өмірдің көптеген салаларында даму мүмкіндіктерін кеңейтеді, бірақ сонымен бірге қауіпсіздікке, соның ішінде жеке деректерді ЖИ-пен өңдеу кезінде қауіп төндіреді. Мақалада жасанды интеллектті дамыту жағдайында дербес деректерді

қорғауды реттеудің құқықтық аспектілері қарастырылады, құпиялылықты қамтамасыз етудің шетелдік тәжірибесі талданады және Қазақстан Республикасындағы жеке деректерді құқықтық қорғаудың қазіргі жағдайы бағаланады.

Зерттеу ЕО, АҚШ, Қытай және Қазақстанның жеке деректерді қорғау саласындағы заңнамасын салыстырмалы құқықтық талдауға негізделген және ЖИ-ті реттеуіндегі айырмашылықтар және осы юрисдикциялардағы құпиялылық құқығын тану дәрежесі талданған. ЕО-да жеке деректер GDPR шеңберінде реттеледі, ол оларды қорғауды жеке тұлғаның ажырамас құқығы ретінде қарастырады. АҚШ-та көзқарас бірыңғай емес және штат деңгейінде айқындалады, бұл құқықтық реттеудің фрагментациясына алып келеді. Қытай, керісінше, деректерді өңдеуді ұлттық қауіпсіздік тұрғысынан бақылайды, бұл азаматтардың жеке деректерін қорғау құқықтарының ауқымын шектейді.

Мақалада Қазақстан Республикасында құқық қолдану практикасының түйінді мәселелері, оның ішінде дербес деректерді қорғау құқығын конституциялық танудың жоқтығы, автоматтандырылған шешімдер қабылдауды реттеудің жеткіліксіздігі және ЖИ қабылдаған шешімдерді «түсіндіру құқығы» тетігінің жоқтығын анықталды. ЖИ шешімдерінің түсіндірілуін қамтамасыз ететін құқықтық нормаларды енгізуді, автоматтандырылған жүйелерде дербес деректерді қорғауды күшейтуді, ұлттық нормаларды халықаралық стандарттармен үйлестіруді қамтитын құпиялылықты қорғауды құқықтық реттеуді жетілдіру бойынша шаралар ұсынылады. Алынған нәтижелер Қазақстанның ЖИ және дербес деректер саласындағы заңнамасын жетілдіру үшін, сондай-ақ цифрлық технологияларды құқықтық реттеу саласындағы одан әрі зерттеулер үшін пайдаланылуы мүмкін.

Түйінді сөздер: жеке деректер, жасанды интеллект, құпиялылық, автоматтандырылған шешім қабылдау, генеративті ЖИ.

© B.A. Umitchinova¹, Y.A. Gavrilova¹, G.A. Menzyuk¹, 2025

¹ Kazakh-American Free University, Ust-Kamenogorsk, Kazakhstan
(E-mail: ¹umitchinova.botagoz@mail.ru; ¹gavriloyuliya@yandex.kz; ¹menzyuk@mail.ru)

LEGAL REGULATION OF PERSONAL DATA IN THE CONTEXT OF ARTIFICIAL INTELLIGENCE DEVELOPMENT: FOREIGN EXPERIENCE AND CHALLENGES FOR KAZAKHSTAN

Abstract. Significant progress in artificial intelligence technologies expands development opportunities in many areas of public life, but at the same time creates security threats, including when AI processes personal data. The article examines the legal aspects of regulating the protection of personal data in the context of the development of artificial intelligence, analyzes foreign experience in ensuring confidentiality and assesses the current state of legal protection of personal data in the Republic of Kazakhstan.

The study is based on a comparative legal analysis of the legislation of the EU, USA, China and Kazakhstan in the field of personal data protection and AI regulation, and analyzes the differences in law enforcement and the degree of recognition of the right to privacy in these jurisdictions. In the EU, personal data is regulated under the GDPR, which views its protection as an inalienable right of the individual. In the United States, the approach is less unified and is determined at the state level, which leads to fragmentation of legal regulation. China, by contrast, controls data processing from a national security perspective, which limits the scope of citizens' rights to protect their personal data.

The article identifies key issues in law enforcement practice in the Republic of Kazakhstan, including the lack of constitutional recognition of the right to personal data protection, insufficient regulation of automated decision-making, and the lack of a mechanism for the "right to an explanation" of decisions made by AI. Measures are proposed to improve the legal regulation of privacy protection, including the introduction of legal norms that ensure the explainability of AI decisions, strengthening the protection

of personal data in automated systems, and harmonizing national norms with international standards. The results obtained can be used to improve the legislation of Kazakhstan in the field of AI and personal data, as well as for further research in the field of legal regulation of digital technologies.

Keywords: personal data, artificial intelligence, privacy, automated decision making, generative AI.

References:

1. Sartor, G. The impact of the General Data Protection Regulation (GDPR) on artificial intelligence. Study Panel for the Future of Science and Technology. EPRS European Parliamentary Research Service // G.Sartor // - Brussels, European Union, 2020. - 84 p. // Retrieved from [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU\(2020\)641530_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf) (date of reference: 15.11.2024).
2. Rajesh, V. Navigating the Privacy Paradox: Balancing AI Advancement and Data Protection in the Digital Age // V.Rajesh, K.Adapa // International Journal of Scientific Research in Computer Science, Engineering and Information Technology. - No10(6). - P. 99-110.
3. Huang, J. Applicable Law to Transnational Personal Data: Trends and Dynamics // J. Huang // German Law Journal. - 2020. - Volume 21. - Issue 6. - P. 1283-1308. // Retrieved from <https://www.cambridge.org/core/journals/german-law-journal/article/applicable-law-to-transnational-personal-data-trends-and-dynamics/28B05974FD63C50F-8BA6EA079B66C6B5> (date of reference: 21.11.2024).
4. Pierre, L. Data Protection in AI-Driven Systems: Understanding the EU's Legal and Regulatory Response Through the General Data Protection Regulation (GDPR) // L. Pierre, U.Barrat // IE University Law School. - June 12th, 2023. // Retrieved from https://www.researchgate.net/publication/385089185_Data_Protection_in_AI-Driven_Systems_Understanding_the_EU's_Legal_and_Regulatory_Response_Through_the_General_Data_Protection_Regulation_GDPR (date of reference: 25.11.2024).
5. Wachter, S. "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation" // S.Wachter, B.Mittelstadt, L.Floridi // International Data Privacy Law. - 2017. - Volume 7. - No2. // Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469 (date of reference: 27.11.2024).
6. King, J. Rethinking Privacy in the AI Era Policy Provocations for a Data-Centric World. // J. King, C.Meinhardt // - Stanford University. White Paper. - February 2024. - 53 p.
7. Clark, J. Europe: The EU AI Act's relationship with data protection law: key take-aways. // J.Clark, M.Demircan, K.Kettas // Retrieved from <https://privacymatters.dlapipiper.com/2024/04/europe-the-eu-ai-acts-relationship-with-data-protection-law-key-take-aways/> (date of reference: 06.12.2024).
8. Mittelstadt, B. AI ethics—too principled to fail? // B. Mittelstadt // Journal of Ethics and Information Technology. - 2019. - No21(4). - P. 345-358 // Retrieved from https://www.researchgate.net/publication/333874695_AI_Ethics_-_Too_Principled_to_Fail (date of reference: 10.12.2024).
9. Binns, R. The lack of comprehensive AI regulation in the US: An overview. // R. Binns // Journal of Technology Law & Policy. - 2022. - No23(1). - P. 45-67.
10. Atata, B. The AI Privacy Paradox: a Comparative Analysis of EU and US Approaches to Regulating Artificial Intelligence and Protecting Personal Data // B.Atata // International Research Journal of Modernization in Engineering Technology and Science. - 2024. - Volume 6. - Issue 9. - P. 1363-1377.
11. Ijaiya, H., Adeniyi, I. AI and Personal Data Privacy in the U.S: Balancing Customer Convenience with Privacy Compliance // H.Ijaiya, I.Adeniyi // ABUAD Law Journal (ALJ). - 2024. Vol. 12. - Issue 1. - P. 41-64. // Retrieved from <https://doi.org/10.53982/alj.2024.1201.03-j> (date of reference: 25.12.2024).
12. Kang, C. How state privacy laws are reshaping the tech landscape // C. Kang // The New York Times. - 2021. // Retrieved from <https://nytimes.com> (date of reference: 30.12.2024).

13. Greenleaf, G. Global data privacy laws 2023: The emerging landscape. Privacy Law & Policy Report. - 2023. // G.Greenleaf // Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4426146 (date of reference: 05.01.2025).
14. Smith, B. The state of AI regulation: Challenges and opportunities // B. Smith // Harvard Law Review. - 2022. - No135(4). - P. 1234-1260.
15. Ratnam, G. Data privacy law seen as needed precursor to AI regulation. // G. Ratnam // Retrieved from <https://rollcall.com/2023/09/26/data-privacy-law-seen-as-needed-precursor-to-ai-regulation/> (date of reference: 10.01.2025).
16. Feng, Y. Personal Data Protection at the Crossroad in China: Legal Framework, Practical Problems and Suggested Reforms // Y.Feng // Asia Pacific Law Review. - 2019. - No27:1. - P. 62-82. // Retrieved from https://www.researchgate.net/publication/334995413_The_future_of_China's_personal_data_protection_law_challenges_and_prospects (date of reference: 13.01.2025).
17. Xiongbiao, Y. Privacy and personal data risk governance for generative artificial intelligence: A Chinese perspective // Y. Xiongbiao, Y. Yuhong, J.Li, B.Jiang // Telecommunications Policy. - 2024. - No48. // Retrieved from <https://doi.org/10.1016/j.tel-pol.2024.102851> (date of reference: 16.01.2025).
18. Chen, Z., et al. Securing privacy in the digital age: The quest for judicial protection of personal information // Z.Chen, R.Geng, Z.Jia, et al. // Journal of Infrastructure, Policy and Development. - 2024. - No8(12). // Retrieved from <https://doi.org/10.24294/jipd.v8i12.9253> (date of reference: 20.01.2025).
19. Yang, L. Practice and Prospect of Regulating Personal Data Protection in China // L.Yang, Y.Lin, B. Chen // Laws. - 2024. - No13. // Retrieved from <https://doi.org/10.3390/laws13060078> (date of reference: 20.01.2025).
20. Gusarova A. Zashchita personalnyh dannyh v Kazahstane 2.0: cifrovoi sled COVID-19. Proekt pri finansovoi podderzhke Fonda Soros-Kazahstan. // A.Gusarova, S. Dzhaksylykov // - 2021. // Retrieved from https://www.soros.kz/wp-content/uploads/2021/03/Personal-Data_Covid-Implications.pdf (data obrashcheniya: 20.03.2025).
21. Tlembaeva Zh.U. O nekotoryh podhodah k pravovomu regulirovaniyu iskusstvennogo intellekta // Zh.U. Tlembaeva // Vestnik instituta zakonodatelstva i pravovoi informatsii Respubliki Kazakstan. - 2021. - №2(65). - S. 61-74.

Авторлар туралы мәліметтер:
Сведения об авторах:
Information about authors:

Умитчинова Ботагоз Аспандиаровна - хат-хабарларға арналған автор, философия докторы (PhD), Қазақстан-Американдық еркін университетінің құқық және халықаралық қатынастар кафедрасының қауымдастырылған профессоры, М. Горький көшесі, 76, 070004, Өскемен, Қазақстан.

E-mail: umitchinova.botagoz@mail.ru; ORCID: <https://orcid.org/0000-0003-4358-4459>; Scopus Author ID: 57697529500.

Гаврилова Юлия Александровна - заң ғылымдарының кандидаты, Қазақстан-Американдық еркін университетінің құқық және халықаралық қатынастар кафедрасының профессоры, М. Горький көшесі, 76, 070004, Өскемен, Қазақстан.

E-mail: gavriloyuliya@yandex.kz; ORCID: <https://orcid.org/0000-0002-1096-4079>; Scopus Author ID: 57191410604.

Мензюк Галина Анатольевна - заң ғылымдарының кандидаты, БҒСБК доценті, Қазақстан-Американдық еркін университетінің құқық және халықаралық қатынастар кафедрасының профессоры, М. Горький көшесі, 76, 070004, Өскемен, Қазақстан.

E-mail: menzjuk@mail.ru; ORCID: <https://orcid.org/0000-0003-4597-7459>.

Умитчинова Ботагоз Аспандиаровна - автор для корреспонденции, доктор философии (PhD), ассоциированный профессор кафедры права и международных отношений Казахстанско-Американского свободного университета, улица М. Горького, 76, 070004, Усть-Каменогорск, Казахстан.

E-mail: umitchinova.botagoz@mail.ru; ORCID: <https://orcid.org/0000-0003-4358-4459>; Scopus Author ID: 57697529500.

Гаврилова Юлия Александровна - кандидат юридических наук, профессор кафедры права и международных отношений Казахстанско-Американского свободного университета, улица М. Горького, 76, 070004, Усть-Каменогорск, Казахстан.

E-mail: gavriloyuliya@yandex.kz; ORCID: <https://orcid.org/0000-0002-1096-4079>; Scopus Author ID: 57191410604.

Мензюк Галина Анатольевна - кандидат юридических наук, доцент ККСОН, профессор кафедры права и международных отношений Казахстанско-Американского свободного университета, улица М. Горького, 76, 070004, Усть-Каменогорск, Казахстан

E-mail: menzjuk@mail.ru; ORCID: <https://orcid.org/0000-0003-4597-7459>.

Umitchinova Botagoz Aspandyarovna - corresponding authors, Doctor of Philosophy (PhD), Associate Professor of the Department of Law and International Relations of the Kazakh-American Free University, 76 M. Gorky Street, 070007, Ust-Kamenogorsk, Kazakhstan.

E-mail: umitchinova.botagoz@mail.ru; ORCID: <https://orcid.org/0000-0003-4358-4459>; Scopus Author ID: 57697529500.

Gavrilova Yuliya Aleksandrovna - Candidate of Law, Professor of the Department of Law and International Relations of the Kazakh-American Free University, 76 M. Gorky Street, 070007, Ust-Kamenogorsk, Kazakhstan.

E-mail: gavriloyuliya@yandex.kz; ORCID: <https://orcid.org/0000-0002-1096-4079>; Scopus Author ID: 57191410604.

Menzyuk Galina Anatolyevna - Candidate of Law, Associate Professor of CCES, Professor of the Department of Law and International Relations of the Kazakh-American Free University, 76 M. Gorky Street, 070007, Ust-Kamenogorsk, Kazakhstan.

E-mail: menzjuk@mail.ru; ORCID: <https://orcid.org/0000-0003-4597-7459>.