

УДК [342.721:004.056]:341.24
DOI: 10.36979/1694-500X-2025-25-11-58-64

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ТРАНСГРАНИЧНОЙ ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ В СТРАНАХ ЕАЭС

А.Ш. Маралбаева

Аннотация. Рассмотрены проблемы и коллизии правового регулирования трансграничной передачи персональных данных в странах ЕАЭС. Развитие мессенджеров, цифровых платформ, онлайн-сервисов, технологий искусственного интеллекта, основанных на больших языковых моделях (Large Language Models, LLM), облачных технологий и трансграничных бизнес-процессов обуславливает необходимость не только национального, но и регионального регулирования вопросов трансграничной передачи персональных данных в современную эпоху цифровой трансформации. Для государств – членов ЕАЭС данная проблема имеет особую актуальность в силу отсутствия наднационального акта ЕАЭС, регулирующего трансграничную передачу персональных данных. Автором было изучено законодательство стран ЕАЭС в сфере трансграничной передачи персональных данных, выявлены проблемы и коллизии правового регулирования и предложены пути их решения.

Ключевые слова: персональные данные; трансграничная передача; законодательство; ЕАЭС.

ЕАЭБ ӨЛКӨЛӨРҮНДӨ ЖЕКЕ МААЛЫМАТТАРДЫ ТРАНСЧЕГАРАЛЫК БЕРҮҮНҮ УКУКТУК ЖӨНГӨ САЛУУ

А.Ш. Маралбаева

Аннотация. ЕАЭБ өлкөлөрүндө жеке маалыматтарды трансчек аралык берүүнү укуктук жөнгө салуунун көйгөйлөрү жана карама-каршылыктары каралат. Мессенджерлерди, санариптик платформаларды, онлайн кызматтарды, чоң тил моделдерине негизделген жасалма интеллект технологияларын (Large Language Models, LLM), булут технологияларын жана трансчек аралык бизнес процесстерин өнүктүрүү санариптик трансформациянын заманбап доорунда жеке маалыматтарды трансчек аралык берүү маселелерин улуттук гана эмес, аймактык жөнгө салууну да талап кылат. ЕАЭБге мүчө мамлекеттер үчүн бул көйгөй жеке маалыматтарды трансчек аралык берүүнү жөнгө салуучу ЕАЭБдин улуттар аралык актынын жоктугуна байланыштуу өзгөчө актуалдуу болуп саналат. Автор ЕАЭБ өлкөлөрүнүн жеке маалыматтарды трансчек аралык берүү жаатындагы мыйзамдарын изилдеп, укуктук жөнгө салуунун көйгөйлөрүн жана карама-каршылыктарын аныктап, аларды чечүү жолдорун сунуштаган.

Түйүндүү сөздөр: жеке маалыматтар; чек ара аркылуу өткөрүү; мыйзамдар; ЕАЭБ.

LEGAL FRAMEWORK OF TRANSBORDER TRANSFER OF PERSONAL DATA IN THE EAEU COUNTRIES

A.Sh. Maralbaeva

Abstract. The article examines the challenges and conflicts of laws in the field of cross-border transfer of personal data in the EAEU countries. The development of messengers, digital platforms, online services, artificial intelligence technologies based on Large Language Models (LLM), cloud technologies and cross-border business processes requires not only national but also regional regulation of cross-border transfer of personal data in the modern era of digital transformation. For the EAEU member states this problem is relevant due to the

lack of the EAEU supranational act regulating the cross-border transfer of personal data. The author examined legislation of the EAEU countries in the field of transborder transfer of personal data, identified problems and conflicts of laws and proposed recommendations.

Keywords: personal data; transborder transfer; legislation; EAEU.

Введение. В странах Евразийского экономического союза (далее ЕАЭС) несмотря на наличие общих подходов к защите персональных данных, подходы к регулированию трансграничной передачи персональных данных имеют существенные различия. Эти различия проявляются в порядке осуществления трансграничной передачи персональных данных, наличии перечня иностранных государств, обеспечивающих адекватный уровень защиты персональных данных, особенностях локализации баз персональных данных и правовых механизмов взаимодействия с иностранными операторами персональных данных.

Интеграция экономических и правовых систем происходит в условиях активного трансграничного взаимодействия граждан, компаний и государственных органов посредством мессенджеров (Whatsapp, Telegram и др.), онлайн-сервисов (торговые цифровые платформы Wildberries, Ozon, Amazon и др.), чат-ботов с искусственным интеллектом (ИИ) (ChatGPT, Gemini, DeepSeek и др.). Странам ЕАЭС необходимо выработать согласованные подходы к трансграничной передаче персональных данных. Отсутствие единых стандартов может не только затруднять трансграничную передачу персональных данных граждан между странами ЕАЭС, но и создавать правовые риски и угрозы для бизнеса, государственных органов и граждан, связанные с нарушением конфиденциальности, утечками персональных данных и кибермошенничеством.

В связи с этим целью настоящего исследования является анализ проблем правового регулирования трансграничной передачи персональных данных с использованием популярных мессенджеров, онлайн-сервисов и чат-ботов с ИИ в странах ЕАЭС и предложение рекомендаций для их решения.

Вопросам изучения правового регулирования трансграничной передачи персональных данных в странах ЕАЭС посвящены труды

А.Н. Артемовой [1], А.Н. Бороздина, В.С. Коварды [2], В.А. Бутич, Т.Н. Михалевой [3], Н.А. Шебановой [4] и др. Вместе с тем следует отметить, что вышеуказанные проблемы правового регулирования трансграничной передачи персональных данных остаются малоизученными.

Методология исследования основана на сравнительно-правовом методе, функциональном анализе и системном подходе.

Трансграничная передача персональных данных в странах ЕАЭС: сравнительно-правовой анализ особенностей правового регулирования

Законы стран ЕАЭС в сфере защиты персональных данных регламентируют правовые основания и порядок трансграничной передачи персональных данных. Правовое регулирование защиты персональных данных в странах ЕАЭС основано на общих принципах законности, конфиденциальности, достоверности, соразмерности и ограничения по хранению персональных данных.

Граждане стран ЕАЭС сталкиваются с трансграничной передачей персональных данных, когда используют популярные мессенджеры (Whatsapp, Telegram и др.), совершают онлайн покупки на сайтах продавцов, находящихся на территории одной из стран ЕАЭС либо другого иностранного государства (Wildberries, Ozon, Amazon и др.), используют чат-боты (например, ChatGPT, Gemini, DeepSeek и др.), размещенные на серверах иностранных государств.

Возникают вопросы: регулируют ли эти повседневные действия законы стран ЕАЭС в сфере защиты персональных данных? Какие правовые последствия предусмотрены для граждан, сотрудников компаний и государственных служащих, использующих Whatsapp, Telegram, ChatGPT, Gemini, DeepSeek в своей профессиональной деятельности для передачи персональных данных?

Под *трансграничной передачей персональных данных* понимается передача персональных

данных на территорию иностранного государства оператором (держателем) персональных данных. Большинство стран ЕАЭС (Армения, Беларусь, Казахстан и Россия) *оператором персональных данных* признают не только государственные органы, муниципальные органы, юридические лица, но и физические лица, если они осуществляют сбор, запись, хранение и др., т. е. обработку персональных данных. Однако в Кыргызстане, в отличие от других стран ЕАЭС, физические лица не признаются держателями (обладателями) персональных данных [5]. В этой связи возникает пробел в праве. Если гражданин Кыргызстана, иностранец, лицо без гражданства, находящиеся в Кыргызстане, самостоятельно осуществляют обработку и передачу персональных данных третьих лиц на территорию иностранного государства, используя популярные мессенджеры (Whatsapp, Telegram, Viber, WeChat и др.), то они не являются субъектами правового регулирования защиты персональных данных. Однако, если организация или индивидуальный предприниматель обязывают клиента или работника отправить свои данные через эти мессенджеры, то Государственное агентство по защите персональных данных при Кабинете Министров Кыргызской Республики может квалифицировать это как трансграничную передачу, так как оператор организует данный процесс.

В Армении, Беларуси, Казахстане и России, если физическое лицо обрабатывает и передает персональные данные третьих лиц, используя популярные мессенджеры Whatsapp, Telegram, Viber, WeChat и др., то оно будет рассматриваться в качестве оператора персональных данных. В этом случае происходит трансграничная передача, так как серверы, через которые происходит передача персональных данных, локализованы в иностранных государствах (США, ЕС, Китай и др.).

С развитием технологий искусственного интеллекта (ИИ) возникают новые вызовы для защиты персональных данных. Доступность, простота и быстрота в использовании популярных моделей генеративного ИИ (ChatGPT, Gemini, DeepSeek и др.) делают их привлекательными для государственных служащих, сотрудников

государственных организаций, бизнес-компаний и студентов. В странах ЕАЭС пока не приняты законы, регулирующие ИИ. В связи с этим, увеличиваются риски утечки персональных данных. К примеру, если государственный служащий загружает документы, содержащие персональные данные третьих лиц в ChatGPT, Gemini, DeepSeek и др. и просит их обработать, то это является трансграничной передачей, так как серверы, на которых обрабатываются персональные данные, находятся в иностранном государстве (США, ЕС, Китае и др.). В этом случае, государственный служащий, действующий от имени государственного органа, выступает оператором (держателем) персональных данных. Он отвечает за сбор, хранение, передачу и защиту персональных данных третьих лиц в соответствии с национальным законодательством. Он должен соблюдать требования национального законодательства в сфере трансграничной передачи персональных данных на территорию иностранного государства. Проблема заключается в том, что в странах ЕАЭС отсутствует единый подход к трансграничной передаче персональных данных.

Сравнительно-правовой анализ позволил выделить сходства и отличия в сфере правового регулирования трансграничной передачи персональных данных в странах ЕАЭС. Во всех странах ЕАЭС на законодательном уровне закреплено, что трансграничная передача персональных данных возможна только в иностранные государства, которые могут обеспечить адекватную защиту прав субъектов персональных данных. Однако национальное законодательство каждой страны ЕАЭС имеет ряд исключений. Рассмотрим их более подробно.

В Республике Армения (РА) условиями трансграничной передачи персональных данных являются: 1) согласие субъекта; 2) если передача данных вытекает из целей обработки личных данных и (или) необходима для реализации этих целей; 3) наличие разрешения Агентства по защите персональных данных Министерства юстиции РА. Такое разрешение требуется, если персональные данные передаются на территорию государства, не обеспечивающего удовлетворительный уровень защиты на основании

договора и договором предусмотрены гарантии защиты персональных данных (статья 27 Закона РА “О личных данных”). Основанием для трансграничной передачи персональных данных, находящихся в распоряжении государственных органов, иностранным государственным органам является наличие международного договора, а негосударственным органам – статья 27 Закона РА “О личных данных” [6].

В Республике Беларусь (РБ) передача персональных данных на территорию иностранного государства, которое не обеспечивает надлежащий уровень защиты прав субъектов персональных данных, возможна только в исключительных случаях. К ним относятся: 1) согласие субъекта персональных данных; 2) наличие договора или международного договора; 3) если передача необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных или иных лиц; 4) если получение согласия субъекта персональных данных невозможно; 5) наличие международных договоров Республики Беларусь; 6) передача осуществляется органом финансового мониторинга в целях принятия мер по предотвращению легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения в соответствии с законодательством; 7) разрешение Национального центра защиты персональных данных РБ (часть 1 статьи 9 Закона РБ “О защите персональных данных”) [7].

В Республике Казахстан (РК) трансграничная передача персональных данных на территорию иностранных государств, не обеспечивающих защиту персональных данных, может осуществляться: 1) только с согласия субъекта (его законного представителя); 2) при наличии международного договора; 3) если это необходимо в целях защиты конституционного строя, охраны общественного порядка, прав и свобод человека и гражданина, здоровья и нравственности населения; 4) для защиты конституционных прав и свобод человека и гражданина, если получение согласия субъекта или его законного представителя невозможно (часть 3 статьи 16 Закона РК “О персональных данных

и их защите”). Трансграничная передача персональных данных может быть ограничена или запрещена законами РК [8].

В Кыргызской Республике (КР) передача персональных данных в страны, не обеспечивающие адекватный уровень защиты прав и свобод субъектов персональных данных, возможна: 1) при наличии согласия субъекта персональных данных на эту передачу; 2) если передача необходима для защиты интересов субъекта персональных данных; 3) если персональные данные содержатся в общедоступном массиве персональных данных (часть 3 статьи 25 Закона КР “Об информации персонального характера”). Кроме этого, при передаче персональных данных по сети Интернет держатель массива персональных данных, передающий такие данные, обязан обеспечить передачу необходимыми средствами защиты, соблюдая при этом конфиденциальность информации [5].

В Российской Федерации (РФ) закреплены два порядка осуществления трансграничной передачи персональных данных: уведомительный и разрешительный [1]. Так, в части 3 статьи 12 ФЗ РФ “О персональных данных” закреплено, что оператор до начала осуществления деятельности по трансграничной передаче персональных данных обязан уведомить Роскомнадзор о своем намерении осуществлять трансграничную передачу персональных данных. Кроме этого, трансграничная передача персональных данных может быть ограничена или запрещена в целях защиты нравственности, здоровья, прав и законных интересов граждан (статья 12 ФЗ РФ “О персональных данных”) [9].

А.Н. Артемова справедливо отмечает, что “серьезную озабоченность вызывает рост случаев утечек персональных данных в результате кибератак” [1]. В целях совершенствования правового регулирования трансграничной передачи персональных данных граждан в Кыргызстане и России были приняты поправки в законодательство.

В 2025 году в Кыргызстане были приняты изменения в Кодекс КР о правонарушениях (далее КоП КР), значительно увеличивающие административные штрафы за трансграничную передачу персональных данных субъектов

персональных данных с нарушением установленного законодательством порядка, если эти действия не содержат уголовно наказуемого деяния. Минимальный штраф для физических лиц составляет 15 000 сомов, для должностных лиц – 17 500 сомов, для юридических лиц – 65 000 сомов. Максимальный штраф для физических лиц – 30 000 сомов, для должностных лиц – 35 000 сомов, для юридических лиц – 100 000 сомов (статья 413³ КоП КР) [10].

В 2022 году в России был принят Федеральный закон РФ (ФЗ РФ) “О персональных данных”, наделяющий его экстерриториальным действием аналогично Общему регламенту по защите данных ЕС (GDPR). Согласно данным поправкам, к обработке персональных данных граждан РФ, осуществляемой иностранными юридическими или физическими лицами, применяются положения ФЗ РФ “О персональных данных” (ч. 1.1. ст. 1 ФЗ «О внесении изменений в Федеральный закон “О персональных данных”») [11]. К примеру, если студенты или работники организации являются гражданами РФ, то университет или работодатель, находящийся в одной из стран ЕАЭС и обрабатывающий их персональные данные, должен будет руководствоваться нормами национального законодательства в сфере защиты и трансграничной передаче персональных данных и ФЗ РФ “О персональных данных”. Однако в этом случае возникает коллизия между национальным законодательством стран ЕАЭС и ФЗ РФ “О персональных данных”. К примеру, статья 1188 Гражданского кодекса КР, регламентирующая защиту личных неимущественных прав иностранных граждан устанавливает, что “к личным неимущественным правам применяется право страны, где имело место действие или иное обстоятельство, послужившее основанием для требования о защите таких прав” [12]. Право на защиту персональных данных является частью права на неприкосновенность частной жизни, которое относится к личным неимущественным правам. Если произошла утечка персональных данных иностранных граждан из-за того, что они были переданы оператором через мессенджеры или чат-боты с ИИ, то в соответствии со статьей 1188 ГК КР при рассмотрении данного дела суд КР будет

применять нормы иностранного государства, где локализованы серверы данных мессенджеров или чат-ботов с ИИ.

В мае 2023 года Роскомнадзор опубликовал Перечень мессенджеров, через которые запрещено передавать платежные документы и персональные данные россиян. В него входят Discord, Snapchat, Skype, Microsoft Teams, Threema, Viber, Whatsapp, WeChat и Telegram [13].

Возрастание рисков и угроз утечки персональных данных и кибермошенничества усиливает необходимость активизации сотрудничества стран ЕАЭС в области защиты прав субъектов персональных данных. Принятие наднационального акта ЕАЭС в сфере защиты персональных данных, включающего сильные стороны законодательства каждой страны ЕАЭС, способствовало бы усилению защиты персональных данных граждан в рамках ЕАЭС. Н.А. Шебанова справедливо отмечает, что на данный момент имеются все предпосылки для разработки такого акта ЕАЭС: внедрение в рамках ЕАЭС интеграционных цифровых платформ, наличие национальных законов о персональных данных в государствах-членах ЕАЭС; осознание объективной необходимости координации усилий для создания нормативной базы, соответствующей потребностям цифровой экономики [4].

Одной из мер по защите персональных данных со стороны государства является принятие Перечня иностранных государств, обеспечивающего адекватную защиту прав субъектов персональных данных (далее – Перечень). В Армении, Беларуси и России такие Перечни приняты. К примеру, в Перечень, принятый Агентством по защите персональных данных Министерства юстиции Республики Армения, вошли 50 государств, обеспечивающих достаточный уровень защиты персональных данных [14]. Основными критериями включения государства в данный Перечень являются: 1) ратификация Конвенции Совета Европы “О защите частных лиц в отношении автоматизированной обработки данных личного характера” (Конвенция 108) или иного международного договора о защите персональных данных; 2) наличие закона о защите персональных данных; 3) наличие уполномоченного государственного

органа по защите персональных данных [14]. В России, согласно Приказу Роскомнадзора от 5 августа 2022 г. N 128 “Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных”, все страны ЕАЭС входят в данный Перечень [15]. В Кыргызстане и Казахстане аналогичные Перечни отсутствуют.

Таким образом, при передаче персональных данных субъектов через популярные мессенджеры и чат-боты с ИИ, оператор обязан убедиться в том, что в иностранном государстве обеспечивается адекватная защита персональных данных, необходимо получить согласие субъекта на такую передачу или иметь правовое основание (договор/международный договор) для трансграничной передачи. В этой связи в странах ЕАЭС необходимо повышать уровень правосознания и цифровой грамотности граждан, государственных служащих, сотрудников бизнес-компаний в сфере трансграничной передачи персональных данных. Передача персональных данных третьих лиц через популярные мессенджеры и чат-боты с ИИ является трансграничной передачей и должна соответствовать требованиям национальных законодательств стран ЕАЭС.

Подводя итог изучению трансграничной передачи персональных данных в странах ЕАЭС, можно сформулировать следующие **выводы**:

Во-первых, несмотря на сходства правового регулирования трансграничной передачи персональных данных, в странах ЕАЭС отсутствует единый подход к данному вопросу.

Во-вторых, сравнительно-правовой анализ национальных законодательств показал, что из всех стран ЕАЭС только ФЗ РФ “О персональных данных” имеет экстерриториальный характер действия в целях защиты персональных данных граждан РФ. Однако это может вызвать коллизии между законами стран ЕАЭС в сфере защиты персональных данных и ФЗ РФ “О персональных данных” в правоприменительной практике. В связи с этим странам ЕАЭС необходимо принять наднациональный акт ЕАЭС в сфере защиты и трансграничной передаче персональных данных [16].

В-третьих, в странах ЕАЭС необходимо повышать уровень правосознания и цифровой

грамотности граждан, государственных служащих, сотрудников бизнес-компаний в сфере трансграничной передачи персональных данных. Популярность бесплатных мессенджеров и чат-ботов с ИИ для передачи персональных данных третьих лиц увеличивает риски их утечки и нарушение прав субъектов персональных данных.

Благодарность. Автор выражает благодарность КРСУ им. Б.Н. Ельцина за финансовую поддержку исследования в рамках Программы развития КРСУ.

Поступила: 29.07.2025;

рецензирована: 12.08.2025; принята: 14.08.2025.

Литература

1. *Артемова А.Н.* Правовое регулирование трансграничной передачи персональных данных / А.Н. Артемова // Юридическая наука и практика. 2023. Т. 19. No 3. С. 9–16. URL: <https://judpract.elpub.ru/jour/article/view/421/236> (дата обращения: 01.12.2024).
2. *Бороздин А.Н.* Анализ системы обеспечения защиты информации в процессе цифровизации ее оборота в рамках ЕАЭС в аспекте повышения экономической безопасности / А.Н. Бороздин, В.В. Коварда // Вестник Евразийской науки. 2020. № 4. URL: <https://esj.today/PDF/41ECVN420.pdf> (дата обращения: 15.12.2024).
3. К вопросу о трансграничной передаче персональных данных из Республики Беларусь // Беларусь в современном мире: материалы XXI Международной научной конференции, посвященной 101-й годовщине образования Белорусского государственного университета, г. Минск, 27 октября 2022 года / редкол.: Е.А. Достанко (гл. ред.) [и др.]. Минск: Белорусский государственный университет, 2022. С. 159–164 (дата обращения: 01.12.2024).
4. *Шебанова Н.А.* Охрана персональных данных в государствах-членах ЕАЭС / Н.А. Шебанова // Журнал Суда по интеллектуальным правам. 2021. Сентябрь. № 3 (33). С. 42–51. URL: <http://ipcsmagazine.ru/legal-issues/protection-of-personal-data-in-the-eaeu-member-states> (дата обращения: 15.12.2024).

5. Закон Кыргызской Республики от 14 апреля 2008 года № 58 “Об информации персонального характера”. URL: <https://cbd.minjust.gov.kg/202269/edition/1239270/ru> (дата обращения: 15.12.2024).
6. Закон Республики Армения от 18 мая 2015 года № ЗР-49-Н “О личных данных”. URL: <https://www.arlis.am/DocumentView.aspx?docid=114851> (дата обращения: 15.12.2024).
7. Закон Республики Беларусь от 7 мая 2021 года № 99-З “О защите персональных данных”. URL: https://pravo.by/upload/docs/op/H12100099_1620939600.pdf (дата обращения: 15.12.2024).
8. Закон Республики Казахстан от 21 мая 2013 года № 94-V “О персональных данных и их защите”. URL: https://online.zakon.kz/Document/?doc_id=31396226&doc_id2=31396226#activate_doc=2&pos=8;-109&pos2=61;-103 (дата обращения: 15.12.2024).
9. Федеральный Закон Российской Федерации от 27 июля 2006 года N 152-ФЗ “О персональных данных”. URL: <https://ivo.garant.ru/#/document/12148567/paragraph/269130:0> (дата обращения: 20.12.2024).
10. Кодекс Кыргызской Республики о правонарушениях от 28 октября 2021 года № 128. URL: <https://cbd.minjust.gov.kg/112306/edition/11339/ru> (дата обращения: 10.07.2025).
11. Федеральный закон «О внесении изменений в Федеральный закон “О персональных данных”», отдельные законодательные акты Российской Федерации о признании утратившей силу части четырнадцатой статьи 30 Федерального закона “О банках и банковской деятельности” от 14 июля 2022 года No 266-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_421898 (дата обращения: 10.07.2025).
12. Гражданский кодекс Кыргызской Республики (часть 2) от 5 января 1998 года № 1. URL: <https://cbd.minjust.gov.kg/5/edition/10133/ru> (дата обращения: 20.12.2024).
13. Информация Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 мая 2023 года “Роскомнадзор назвал мессенджеры, запрещенные для передачи платёжных документов и персональных данных россиян”. URL: <https://www.garant.ru/hotlaw/federal/1623238/> (дата обращения: 10.07.2025).
14. Министерство юстиции Республики Армения. Установлен список стран, обеспечивающих достаточный уровень защиты персональных данных. URL: <https://www.moj.am/ru/article/1731> (дата обращения: 20.12.2024).
15. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 5 августа 2022 года N 128 “Об утверждении перечня иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных”. URL: <https://ivo.garant.ru/#/document/405309273/paragraph/2:0> (дата обращения: 20.12.2024).
16. *Маралбаева А.Ш.* Унификация национальных законодательств стран ЕАЭС в сфере защиты персональных данных: проблемы и перспективы / А.Ш. Маралбаева // Вестник КРСУ. 2024. Т. 24. № 11. С. 110–117. URL: <http://vestnik.krsu.edu.kg/archive/207/8263> (дата обращения: 10.07.2025).