Научная статья
УДК 34:004:342.721:004.8
EDN: https://elibrary.ru/ppljhu
DOI: https://doi.org/10.21202/jdtl.2024.15

Правовые проблемы трансграничной передачи данных в эпоху цифровизации государственного управления

Гульбакыт Болатбеккызы

Уханьский университет, Ухань, Китай

Ключевые слова

государственное управление,
защита данных,
кибербезопасность,
конфиденциальность,
персональные данные,
права человека,
право,
трансграничность,
цифровизация,
цифровые технологии

Аннотация

Цель: определить основные юридические факторы трансграничного обмена данными в контексте распространения цифровых технологий и цифровизации государственного управления, включая правовые гарантии, проблемы безопасности, риски кибербезопасности, подходы к регулированию и повышению эффективности управления данными в разных юрисдикциях.

Методы: исследование опирается на синтез и критический анализ различных аспектов заявленной проблемы, в том числе на анализ как первичных, так и вторичных источников. На примере сравнения политики регулирования Китая, США, ЕС и государств-членов ЕАЭС сопоставляются различные подходы относительно ограничения или поощрения свободной трансграничной передачи данных. Комплексный мета-анализ и оценка литературы позволили сформировать представление о методах, используемых для защиты данных в разных юрисдикциях, а также обозначить рамки и направления государственной политики, необходимые для эффективной передачи данных между юрисдикциями.

Результаты: выявлены основные проблемы, связанные с трансграничной передачей данных в контексте распространения цифровых технологий и цифровизации управления, такие как растущее неравенство в развитии цифровых технологий, правовая неопределенность, обеспечение конфиденциальности и кибербезопасности и др. Проанализированы правовые основы трансграничной передачи данных в контексте цифровизации государственного управления и практика их реализации, что способствовало поиску путей повышения эффективности управления в условиях транснациональной передачи данных, включая предоставление услуг, развитие открытости и участия общественности.

Научная новизна: на основе проведенного анализа подходов различных юрисдикций к проблемам юридического характера, вопросам обеспечения безопасности и суверенитета, обусловленным трансграничной передачей данных, выявлены роль и применимость международного права, а также уникальные вызовы, возникающие в государствах-членах Евразийского экономического союза на пути формирования трансграничного пространства доверия.

Практическая значимость: исследование указанных вопросов имеет значение для выработки и принятия взвешенных политико-правовых решений государственными структурами, прежде всего правительственными и законодательными органами, направленных на достижение баланса между доступностью данных и их безопасностью, между эффективностью государственного управления и соблюдением прав граждан. Полученные результаты будут иметь значение также для иных субъектов отношений, связанных с трансграничной передачей данных и вопросами регулирования указанных отношений.

Для цитирования

Болатбеккызы, Г. (2024). Правовые проблемы трансграничной передачи данных в эпоху цифровизации государственного управления. *Journal of Digital Technologies and Law*, *2*(2), 286–307. https://doi.org/10.21202/jdtl.2024.15

Содержание

Введение

Трансграничная передача данных в контексте цифровизации управления подразумевает передачу персональных или конфиденциальных данных через государственные границы для достижения различных целей, включая оказание государственных услуг, развитие международных партнерских отношений и обмен данными между государственными учреждениями и частным сектором. Передача данных через границы в рамках цифровизации управления необходима для повышения качества государственных услуг и развития международного сотрудничества. Эта практика играет важную роль в развитии как государственных услуг, так и глобального сотрудничества.

Однако при этом возникают проблемы юридического характера, вопросы безопасности и суверенитета, которые необходимо решать на основе международных соглашений и надежных мер в области защиты данных. Достижение баланса между доступностью и безопасностью данных – сложная задача, требующая от правительств тщательной работы по соблюдению прав граждан и международных правовых рамок.

Кроме того, в настоящее время не существует ни одного закона или нормативного акта, касающегося трансграничной передачи или регулирования данных, который мог бы быть согласован на глобальном уровне и единогласно одобрен членами международного сообщества. Ситуация усугубляется из-за растущего неравенства в распространении цифровых технологий, которые до сих пор не доступны в равной степени для всех стран, независимо от их ВВП.

1. Трансграничная передача данных и ее значение для цифровизации государственного управления

1.1. Категоризация трансграничной передачи данных

Выделяют четыре основные категории трансграничной передачи данных. Во-первых, это межправительственный обмен данными (Government to Government, G2G), то есть обмен данными между государственными структурами отдельных стран, служащий таким целям, как дипломатическое сотрудничество, координация действий правоохранительных органов и реагирование на стихийные бедствия. Это общепринятая практика, когда международные правоохранительные органы обмениваются данными для борьбы с глобальной преступностью. Например, Европол призван способствовать обмену информацией между европейскими правоохранительными органами для борьбы с организованной преступностью и терроризмом (De Moor & Vermeulen, 2010). Во время международных кризисов правительства сотрудничают друг с другом, обмениваясь данными для управления мероприятиями по ликвидации последствий стихийных бедствий и оказанию гуманитарной помощи. Например, Управление ООН по координации гуманитарных вопросов (Office for the Coordination of Humanitarian Affairs, OCHA) способствует обмену данными во время чрезвычайных гуманитарных ситуаций (Bennett, 2002).

Вторая категория – это обмен данными между правительством и бизнесом (Government to Business, G2B), в ходе которого государственные структуры передают данные организациям частного сектора для содействия сотрудничеству между государственным и частным секторами или в целях приватизации государственных

функций (например, передача налогового администрирования частным компаниям). Для обеспечения беспрепятственного транзита товаров через международные границы государственные структуры и таможенные органы обмениваются данными, относящимися к международной торговле и таможне, включая данные об отправлениях и грузовых декларациях. Чтобы исключить двойное налогообложение компаний и частных лиц, налоговые органы разных стран могут обмениваться информацией о налогоплательщиках в рамках соглашений о предупреждении двойного налогообложения (Niu et al., 2021).

Третье направление – обмен данными между правительством и частными лицами (Government to Citizen, G2C). Это трансграничная передача данных граждан для получения международных услуг (например, доступа к медицинскому обслуживанию за рубежом). Когда граждане одной страны выезжают за границу, их медицинские карты могут быть доступны на международном уровне для обеспечения соответствующего медицинского обслуживания. Например, инфраструктура цифровых услуг электронного здравоохранения Европейского союза (eHealth Digital Service Infrastructure, eHDSI) позволяет гражданам ЕС получать доступ к медицинским данным во время поездок по территории ЕС (Bruthans & Jiráková, 2023).

Правовая база и соответствующая практика играют важную роль при трансграничной передаче данных в цифровом управлении; сюда включаются законы о защите данных и международные соглашения в этой области. Согласно законам о защите данных их передача должна осуществляться в соответствии с правилами защиты данных как страны происхождения, так и страны-получателя. В качестве примера можно привести Общий регламент Европейского союза по защите данных, который устанавливает строгие требования к трансграничной передаче данных, уделяя особое внимание определению соответствия стандартным условиям договора и обязательным корпоративным правилам. Стоит упомянуть и Китайский закон о защите личной информации (Personal Information Protection Law, PIPL), который также имеет экстерриториальное действие и устанавливает требования как для государственного, так и для негосударственного сектора. Что касается международных соглашений, то между некоторыми странами заключены двусторонние соглашения, регулирующие передачу данных. В частности, таковой являлась Программа по защите конфиденциальности ЕС–США (EU-U.S. Privacy Shield), которая способствовала обмену данными между ЕС и США, пока не была отменена в результате рассмотрения дела Schrems II.

Вопросы суверенитета и локализации данных становятся одними из самых сложных в области трансграничной передачи данных. Некоторые страны вводят требования по локализации данных, согласно которым определенные категории данных должны храниться на их территории. Например, согласно российским нормам, персональные данные российских граждан должны храниться на серверах, расположенных на территории России (Gurkov, 2021). Другой пример – недавняя ситуация с российским филиалом Yandex.kz в Казахстане[1], когда министерства и представители компании Yandex приняли решение о физическом переносе серверов в Казахстан после инцидента с блокировкой сайта на территории Казахстана из-за нежелания компании соблюдать условия соглашения.

[1] «Яндекс» переносит свою инфраструктуру в Казахстан под угрозой блокировки. (2023, 21 августа). CNews. https://clck.ru/39o7xf

При передаче данных через границы стран одинаково важны безопасность и кибербезопасность. Данные должны быть защищены от нежелательного доступа или утечки. Чтобы гарантировать конфиденциальность и безопасность передаваемых данных, необходимо использовать шифрование, безопасные протоколы и надежные меры кибербезопасности.

Повышение качества государственных услуг и развитие международного сотрудничества в рамках цифровизации государственного управления требуют трансграничного обмена данными. Однако при этом возникают проблемы, связанные с суверенитетом, безопасностью и правом, которые должны быть решены с помощью международных соглашений и надежных протоколов защиты данных. Поиск баланса между доступностью и безопасностью данных – сложный процесс, требующий от правительств осторожности при соблюдении прав своих граждан и следовании международным правовым нормам.

1.2. Проблемы конфиденциальности и безопасности данных при их трансграничной передаче

Трансграничная передача данных в контексте цифровизации управления вызывает серьезные опасения в отношении конфиденциальности и безопасности данных. Эти опасения обусловлены различными факторами, включая правовые гарантии, проблемы безопасности, риски кибербезопасности, сложности юрисдикции, сложность законодательных решений и необходимость надежного управления данными. Эффективное решение этих проблем требует внедрения правовых протоколов, тактик кибербезопасности и процедур управления данными, направленных на защиту частной информации граждан в условиях все большего распространения цифровых технологий.

По мере развития новых передовых технологий граждане ожидают все более продвинутых услуг и улучшения различных аспектов жизни. Технологический прогресс позволяет находить более эффективные решения существующих проблем, но при этом возникают новые проблемы, связанные с безопасностью и неприкосновенностью частной жизни. Цифровизация информационных ресурсов создает дополнительные проблемы в области цифровых данных и инфраструктуры. В то время как развитые страны внедряют надежные меры безопасности и методы оптимизации, развивающиеся страны по-прежнему сталкиваются с трудностями в решении этих вопросов[2].

Трансграничная передача данных предполагает соблюдение правовых норм и требований, необходимых для беспрепятственного перемещения данных. Эти нормы распространяются как на передачу данных внутри организации, работающей вне национальных границ, так и на передачу данных между организациями в разных странах. Например, во многих юрисдикциях, включая ЕС, Великобританию и Китай, установлено требование, согласно которому для обеспечения безопасной и законной передачи данных из одной страны в другую страна-получатель должна обеспечивать стандарты конфиденциальности личной информации, как минимум, эквивалентные

[2] UNGA. Nearly Half of the World's Population is Excluded from 'Benefits of Digitalization', the Speaker stresses as the Second Committee Debates Information Technology for Development. https://clck.ru/39o86M

стандартам страны-отправителя. Только в этом случае орган регулирования конфиденциальности данных или иной орган управления (в ЕС это Европейская комиссия) может вынести решение, позволяющее беспрепятственно передавать данные через границы.

2. Обеспечение безопасности и эффективности при трансграничной передаче данных

2.1. Механизмы обеспечения безопасности трансграничной передачи данных

Для того чтобы всесторонне осветить современную ситуацию с безопасностью при трансграничной передаче данных, рассмотрим практику применения различных норм. Хотя глобальной системы сертификации адекватности защиты данных при их трансграничной передаче не существует, многие страны и региональные группы стран внедрили свои собственные правила и положения для контроля в этой области. Выделяют пять самых распространенных подходов:

1. Заключения о признании адекватности защиты: передача данных разрешена в регионы, в которых, согласно заключению государственных органов, стандарты защиты данных соответствуют или превосходят стандарты страны происхождения. Общий регламент ЕС по защите данных гласит, что за выдачу заключений об адекватности защиты отвечает Европейская комиссия. Исследование, проведенное Международной ассоциацией специалистов в области защиты информации (International Association of Privacy Professionals, IAPP), показало, что в 74 юрисдикциях принята норма, по которой государственные организации, такие как регуляторы конфиденциальности данных или иные правительственные структуры, уполномочены выдавать заключения об адекватности защиты при передаче данных[3]. Важно понимать, что эти заключения не всегда являются окончательными и могут быть пересмотрены в связи с изменением обстоятельств или модификацией законов о защите данных.

2. Договорные соглашения: договоры о передаче данных используются для авторизации передачи данных за пределы юрисдикции, в которой находится организация. Такие договоры гарантируют строгое соблюдение соответствующих стандартов соответствия, например, в области обработки и хранения данных. На практике наиболее часто используются стандартные договорные положения (Standard Contractual Clauses, SCC). Это заранее составленные положения, которые включаются в договоры между импортерами и экспортерами данных для их трансграничной передачи. Они были одобрены Европейской комиссией как соответствующие Общему регламенту ЕС по защите данных. По оценке IAPP, в настоящее время 71 страна мира использует стандартизированные договорные положения[4].

3. Правила передачи данных внутри организации, или обязательные корпоративные правила (Binding Corporate Rules, BCR), представляют собой совокупность внутренних политик и соглашений, регулирующих защиту данных и авторизующих трансграничную передачу данных в рамках одной организации. BCR признаются в различных юрисдикциях, включая ЕС, Великобританию, Бразилию, Сингапур и Южную Африку.

---

3 International Association of Privacy Professionals. Infographic: Global Adequacy Capabilities. https://clck.ru/39o88u

4 Там же.

Многие организации отдают предпочтение BCR Евросоюза, чтобы структурировать свои глобальные проекты при соблюдении конфиденциальности данных. Однако внедрение BCR может быть сложным и трудоемким процессом, поскольку для этого необходимо получить разрешение соответствующих органов по защите данных.

4. Механизмы сертификации: несколько юрисдикций признают сертификаты по передаче данных, выданные соответствующими органами. Чтобы получить сертификат, компания должна пройти проверку со стороны независимого контролирующего органа (Accountability Agent, AA), который может быть как государственной структурой, так и частной организацией. В настоящее время единственным таким механизмом является система трансграничных правил конфиденциальности АТЭС (Cross-Border Privacy Rules, CBPR), признанная в восьми странах: Австралии, Канаде, Китае, Японии, Южной Корее, Мексике, Сингапуре и США.

5. Согласие пользователя: несмотря на сложности масштабирования, получение согласия пользователя традиционно служит основным подходом к трансграничной передаче данных. Оно особенно широко применяется в сложных правовых средах, где является центральным элементом различных режимов передачи данных. Согласие пользователя должно соответствовать определенным критериям, в том числе быть информированным, явным и недвусмысленным, при этом стандарты получения согласия в разных юрисдикциях различны. Согласно Общему регламенту ЕС по защите данных, согласие пользователя может служить механизмом обеспечения передачи данных только в том случае, если не имеется Заключения о признании адекватности защиты или других гарантий, таких как стандартные договорные положения или обязательные корпоративные правила. Отсутствие общепринятых норм сертификации адекватной защиты данных затрудняет для организаций навигацию по сложному ландшафту нормативных актов в этой области.

В связи с этим правительства многих стран активно пытаются решить проблему трансграничной передачи данных. Совместными усилиями они стремятся создать благоприятные условия для законных трансграничных потоков данных, обеспечивая при этом защиту конфиденциальности личной информации и безопасности данных.

2.2. Правительственные инициативы для повышения эффективности трансграничной передачи данных

Рассмотрим ряд недавних инициатив, предпринятых правительствами отдельных стран для повышения эффективности трансграничной передачи данных.

Европейский союз и Соединенные Штаты совместно представили новый рамочный документ ЕС–США о конфиденциальности данных Data Privacy Framework (DPF)[5]. Он заменяет прежнюю Программу по защите конфиденциальности ЕС–США (EU-U.S. Privacy Shield), которая была отменена в результате решения по делу Schrems II в 2020 г. Европейской комиссии было дано указание не утверждать рамочный документ до тех пор, пока в нем не будут адекватно устранены опасения, высказанные в деле Schrems II как Парламентом ЕС, так и Советом ЕС по защите данных (Gao & Chen, 2022).

[5] International Association of Privacy Professionals. (n.d.). EU-U.S. Data Privacy Framework: Guidance and Resources. https://clck.ru/39o8Dg

По инициативе Японии правительства стран Большой семерки активно развивают институциональное партнерство (Institutional Arrangement for Partnership, IAP)[6]. Оно призвано восполнить пробел в создании эффективного и надежного механизма международного сотрудничества для введения в действие системы «Свободный поток данных на основе доверия» (Data Free Flow with Trust, DFFT).

С 1 июня 2023 года в Китае введены в действие Правила заключения стандартного договора о трансграничной передаче персональных данных. Они обязывают организации, обрабатывающие персональные данные (даже те, что обрабатывают данные менее 1 миллиона человек), заключать договоры с зарубежными получателями данных перед их передачей за границу. Законодательство Китая по обеспечению безопасности данных включает в себя три ключевых закона: Закон о кибербезопасности, Закон о безопасности данных и Закон о защите персональной информации. Эти законы подкреплены целым рядом правительственных постановлений. В соответствии с этими актами центральное правительство сформировало систему регулирования экспорта персональных данных.

Кроме того, был проведен форум, посвященный системе трансграничных правил конфиденциальности (Global Cross-Border Privacy Rules, CBPR) (Joel, 2023). Страны-члены Азиатско-Тихоокеанского экономического сотрудничества (АТЭС), включая США, Канаду, Японию, Сингапур и другие государства, инициировали этот форум с целью создания международной системы сертификации на основе CBPR и соответствующих систем признания конфиденциальности при обработке информации (Privacy Recognition for Processors, PRP).

В условиях стремительной трансформации цифровой экономики организации должны сохранять гибкость и активно обновлять свои методы и протоколы в соответствии с постоянно меняющейся нормативно-правовой базой. Это особенно важно для крупных организаций, ведущих обширную деятельность во всем мире, поскольку несоблюдение требований может привести к значительным штрафам. Например, в 2021 г. европейские органы надзора за защитой данных наложили штрафы на сумму около 1,2 млрд долларов США, причем самый крупный штраф выплатил американский онлайн-ритейлер[7]. В 2022 г. Управление по киберпространству Китая (China's Cyberspace Administration, CAC) оштрафовало известную компанию Didi Global (сервис по заказу такси) на 8 млрд юаней (1,2 млрд долларов) за нарушение правил национальной безопасности и защиты персональных данных. Китайские компании, расположенные на территории страны и планирующие первичное размещение акций на международном рынке, до сих пор сталкиваются с последствиями этого решения[8].

При наличии различных механизмов для облегчения трансграничной передачи данных каждая организация должна самостоятельно оценивать и выбирать наиболее подходящие варианты, исходя из своих конкретных потребностей. Универсального

---

6 World Economic Forum. (2023, April 26). How and why data must flow freely and responsibly across borders. https://clck.ru/39o8Gf

7 EDPB. (2023, May 22). 1.2 billion euro fine for Facebook as a result of EDPB binding decision. https://clck.ru/39o8HK

8 Webster, G. (2022, July 21). Chinese Authorities Announce $1.2B Fine in DiDi Case, Describe 'Despicable' Data Abuses. DigiChina. https://clck.ru/39o8KA

решения не существует. В зависимости от ситуации правительства могут использовать одновременно несколько систем. Также важно, чтобы меры по авторизации передачи данных были органично интегрированы в существующие рабочие процессы. Отсутствие эффективных мер может привести к необходимости длительных и дорогостоящих согласований в различных инстанциях.

3. Применимость международного права для регулирования трансграничной передачи данных

3.1. Подходы различных юрисдикций к проблеме трансграничной передачи данных

Очевидно, что роль международного права в регулировании трансграничной передачи данных весьма велика; оно служит краеугольным камнем в деле защиты частной жизни, соблюдения прав человека, обеспечения кибербезопасности, содействия торговле, урегулирования конфликтов и создания индивидуальных соглашений. Оно закладывает основу и определяет стандарты надлежащего управления данными на международном уровне, способствует ответственной реализации такого управления и укрепляет доверие к цифровым взаимодействиям.

Как отмечалось, интернет «не поддается регулированию». Однако в Интернете стираются границы между национальными государствами, но не законы (Chuanying, 2020). В совместном исследовании, проведенном по заказу Министерства обороны в 1998 г., отмечается следующее.

Возможно, реальная проблема, с которой сталкиваются правительства в связи с развитием Интернета (и других средств коммуникации с использованием информационных технологий), заключается не столько в распространении информации, сколько в увеличении числа участников на уровне правительств и дипломатии. Организованные группы и отдельные лица могут создавать (и фактически создают) коалиции как внутри страны, так и на международном уровне, которые оказывают беспрецедентное давление на национальные правительства в отношении практически любой деятельности или сферы интересов. Эти группы могут фактически создавать то, что правительствам остается только признать. В связи с этим возникает вопрос, изменилась ли природа суверенитета после возникновения возможности мгновенных и повсеместных коммуникаций, и если да, то как (Press et al., 1998).

Иного мнения придерживается доцент Мэрилендского университета в Колледж-Парке, доктор Вирджиния Хауфлер (Virginia Haufler): «Разработку и внедрение эффективных норм на основе директивных, правительственных подходов затрудняет децентрализованный, открытый, глобальный характер… Интернета» (Haufler, 2013).

Разрушительные террористические атаки 11 сентября и использование террористами Интернета для коммуникации послужили толчком к принятию развитыми странами мер по ограничению контента. По данным общественной организации, выступающей за свободу журналистики, еще в сентябре 2002 г. США, Великобритания, Франция, Германия, Испания, Италия, Дания, Европейский парламент, Совет Европы и страны Большой восьмерки выражали обеспокоенность по поводу своих прав и свобод в Интернете (Nijboer, 2004).

Международные правительственные организации столкнулись с серьезными проблемами в связи с тем, что цели государств при ограничении контента существенно

различаются. Эти разногласия стали очевидными на открытии Всемирной встречи на высшем уровне по вопросам информационного общества (World Summit for the Information Society, WSIS) в декабре 2003 г. Одними из ключевых разногласий в ходе переговоров на этом форуме стали формулировки, используемые для рассмотрения последствий высказываний в Интернете. Китай, что немаловажно, выразил свое отрицательное отношение к тексту о свободе прессы, который отражал американскую точку зрения. В результате в Декларации принципов свобода прессы все же была упомянута, но в более сдержанной форме и с добавлением формулировки, подчеркивающей важность национального суверенитета (Berleur, 2007)[9]. Принятый План действий гласил, что правительства должны принять необходимые меры для борьбы с вредным и незаконным медиаконтентом, соблюдая при этом право на свободу слова (Jensen, 2006). Внешние наблюдатели сошлись во мнении, что План действий игнорирует непримиримые разногласия по регулированию контента и дает мало указаний на будущее (Souter, 2004).

К примеру, Соединенные Штаты и Евросоюз по-разному относятся к конфиденциальности данных. Американская позиция в отношении личных прав базируется в основном на идее невмешательства государства. В результате в США не получили особой поддержки законы штатов, касающиеся конфиденциальности данных. Как отмечают Bessette and Haufler (2001), в США предпочитают скорее рыночный метод сбора данных. «Если на международном уровне будут приняты законы о неприкосновенности частной жизни, то они, естественно, станут преобладающим методом ее обеспечения», – заявил представитель администрации президента Айра Магазинер (Farrell, 2003).

В Европе, напротив, тайна частной жизни рассматривается как одно из фундаментальных прав, которое должно находиться под защитой государства. Bessette and Haufler отмечают, что «европейские страны, в частности, ввели надежные гарантии неприкосновенности частной жизни, определив ее как одно из основных прав человека» в результате случаев нарушения неприкосновенности частной жизни со стороны правительства (Mai'a, 2023). В 1995 г. Европейский союз принял всеобъемлющую Директиву о защите данных, которая установила для европейских компаний четкие правила и механизмы их соблюдения. Директива была направлена на предотвращение деятельности компаний за пределами юрисдикции ЕС в целях обхода закона. Она запрещала передавать личные данные граждан ЕС странам, не обеспечивающим надлежащую безопасность. Директива должна была вступить в силу в конце 1998 г. (Long & Quek, 2002).

Учитывая масштабы этого запрета, Австралия, Канада и страны Восточной Европы были вынуждены изменить свои собственные правовые системы, чтобы соответствовать стандартам ЕС. США, однако, предприняли ответные меры, вынудив американские транснациональные корпорации создать системы саморегулирования, соответствующие законам ЕС.

Тоталитарные режимы использовали простые, но эффективные методы регулирования интернет-контента. Предпринимались такие меры, как ограничение использования персональных компьютеров, контроль и запрет нежелательного контента

[9] McCarthy, K. (2003, December 8). Internet Showdown Side-stepped in Geneva. The Register Newsletter, 8. https://clck.ru/39o8LW

(порнографических материалов, аморальных сайтов, религиозного и политического контента), что в конечном итоге привело к цензурированию Интернета и широкому использованию систем фильтрации контента (Drezner, 2004).

В научной литературе, посвященной глобализации, часто чрезмерно упрощают сложную систему управленческих взаимодействий в международной политике, фокусируясь исключительно на бинарной оппозиции между государственной и негосударственной властью. Более верное представление о последствиях глобализации можно получить, признав возможность существования различных механизмов глобального управления. Изучение управления Интернетом показывает, что правительства могут вмешиваться в ситуацию, когда это необходимо для достижения их собственных целей, даже если ранее они возложили управленческие обязанности на коммерческие организации.

Если крупные державы не могут наладить сотрудничество, а другие международные игроки поддерживают какую-либо из влиятельных стран, то возникают так называемые «конкурирующие стандарты». В ходе исследований были выявлены два примера таких стандартов: это защита конфиденциальности данных и регулирование генетически модифицированных организмов (Trump et al., 2023). В обоих случаях США и ЕС продвигают свои системы норм для регулирования этих вопросов. Обеим сторонам удалось заручиться определенной поддержкой, однако ни один из стандартов не достиг всеобщего признания.

Наконец, предполагается, что если крупные державы придут к согласию, но их интересы не совпадут с интересами других международных игроков, то в результате появятся «клубные стандарты». Эти стандарты представляют собой одну из самых захватывающих сторон регулирования. В этом сценарии влияние крупных держав становится очевидным, поскольку они оказывают давление на другие государства и ведут с ними переговоры о создании стандарта. Часто все начинается с небольшой, но влиятельной группы, такой как ОЭСР или Целевая группа по борьбе с отмыванием преступных доходов. Эти коалиции государств-единомышленников могут выработать системы норм и впоследствии убедить другие государства принять их.

3.2. Программа по защите конфиденциальности ЕС–США и ее влияние на трансграничную передачу данных между ЕС и США

Программа по защите конфиденциальности ЕС–США – это система, призванная регулировать передачу персональных данных из Евросоюза в Соединенные Штаты. Ее основной целью было обеспечить соблюдение европейских правил защиты данных при их передаче. После того как Европейский суд отменил концепцию «Безопасной гавани» в результате решения по делу Schrems I, принятого в 2015 г., в 2016 г. была введена новая структура. Ее главной целью было создание правовой базы для передачи персональных данных из ЕС в США и обеспечение соблюдения американскими организациями стандартов защиты данных, сопоставимых с теми, что действуют в ЕС.

По мнению Европейской комиссии, Программа по защите конфиденциальности ЕС–США обеспечивает приемлемый уровень защиты данных в США, поэтому система защиты данных ЕС получила «заключение об адекватности». При определении уровня защиты должны были учитываться все соответствующие аспекты операции по передаче данных или серии связанных между собой действий.

При этом учитывалось множество переменных, в том числе «правовые нормы, как общие, так и специфические для третьей страны, а также профессиональные стандарты и меры безопасности, принятые в этой стране» (Hijmans, 2006).

Чтобы предотвратить обработку данных компаниями за пределами ЕС с целью обойти Директиву 1995 г., было введено ограничение на передачу данных (Drezner, 2008). Ряд стран изменили свое законодательство в попытке достичь стандартов адекватности. Однако вместо того, чтобы поддерживать законодательные меры, имеющие обязательную силу, Соединенные Штаты поддержали варианты саморегулирования, которые соответствовали саморегулируемому характеру федеральной политики в области конфиденциальности данных (Voss, 2019).

Сравнению подходов США и ЕС к разработке политики регулирования Интернета посвящены многочисленные исследования. Результаты показывают, что ЕС обычно разрабатывает широкое и всеобъемлющее законодательство. Однако эта законодательная процедура часто продвигается медленнее, что представляет проблему, особенно когда речь идет о быстрой эволюции Интернета и новых технологиях. В США, напротив, разработана более децентрализованная нормативная база с множеством агентств и иногда несовместимыми между собой нормативными актами (Reidenberg, 1996).

Существенные разногласия между ними усугубляются различиями между данными и метаданными. Федеральное законодательство США предоставляет правоохранительным органам значительные полномочия по доступу к метаданным (Schneider, 2009).

Однако в отношении Программы по защите конфиденциальности ЕС–США Европейский суд признал решение Европейской комиссии № 2016/1250 незаконным. По мнению суда, это решение не гарантировало степень защиты персональных данных, эквивалентную той, которая требуется согласно европейскому законодательству (Furramani, 2023).

В 2016 г. было принято решение Европейской комиссии № 2016/1250, которое разрешило передачу персональных данных из ЕС в США. В результате компании из ЕС и Европейской экономической зоны отправляли персональные данные американским организациям, включенным в список Программы по защите конфиденциальности ЕС–США, с особыми гарантиями защиты данных (Furramani, 2023).

Указанное дело было инициировано гражданином Австрии, пользователем Facebook[10], который возражал против передачи своих данных в США, заявляя, что США не обеспечивают такого же уровня защиты, как требуется по законодательству ЕС. В 2013 г. он подал иск, который комиссар по защите данных первоначально принял к рассмотрению[11]. После повторного изучения материалов комиссар пришел к выводу, что передача персональных данных в США не соответствует статьям 7, 8 и 47 Европейской хартии о правах человека[12]. Это послужило поводом для передачи дела в Верховный суд.

[10] Организация признана экстремистской, ее деятельность запрещена на территории Российской Федерации.

[11] CJEU, Schrems II, 2020, July 16, paras 50, 51 and 52.

[12] CJEU, Schrems II, 2020, July 16, paras 55 and 56.

По мнению Верховного суда, США не обеспечили адекватную защиту личной информации в соответствии со статьями 7 и 8 Хартии ЕС о правах человека. Суд выявил несколько проблем, включая применение Четвертой поправки к гражданам Европы, сомнения по поводу деятельности Агентства национальной безопасности без судебного надзора, а также несоответствия между положением об омбудсмене Программы по защите конфиденциальности ЕС–США и статьей 47 Хартии. В связи с этим Верховный суд передал дело в Европейский суд[13].

Согласно статье 45 Общего регламента по защите данных, Европейский суд постановил, что передача личной информации из ЕС или ЕАЭС в третьи страны должна быть основана на адекватном решении, принятом Комиссией. Если такое решение не принято, данные могут быть переданы при условии «надлежащих гарантий» согласно статье 46 Общего регламента по защите данных, которая определяет права субъектов и средства правовой защиты[14].

Суд подчеркнул роль национальных надзорных органов в отношении защиты личной информации в соответствии со статьями 51(1) и 57(1) Общего регламента по защите данных. Он указал, что национальные органы власти отвечают за соблюдение норм, установленных нормативными актами ЕС, при передаче персональных данных из ЕС или Европейской экономической зоны в другие страны или международные организации[15, 16].

Национальные надзорные органы должны иметь возможность рассматривать иски и оценивать соответствие переданных данных положениям Общего регламента даже в тех случаях, когда Европейская комиссия утвердила заключение об адекватности защиты, разрешающее передачу личной информации[17, 18].

По мнению Европейского суда, Программа по защите конфиденциальности ЕС–США не гарантирует прав субъектов данных, как требует Хартия Евросоюза о правах человека. Право на справедливое судебное разбирательство и эффективные средства правовой защиты гарантируются Хартией. Кроме того, Европейский суд постановил, что в соответствии со статьей 47 Хартии омбудсмен по вопросам Программы по защите конфиденциальности ЕС–США, назначаемый государственным секретарем, не относится к категории автономной организации или судебного органа[19].

По сути, Европейский суд пришел к выводу, что США не обеспечивают уровень защиты данных, эффективно сопоставимый с уровнем защиты Европейского союза, как того требует статья 45(1) Общего регламента по защите данных с учетом статей 7, 8 и 47 Хартии. Эти статьи гарантируют право на эффективную правовую защиту, уважение частной и семейной жизни, а также защиту персональных данных. В результате заключение об адекватности защиты было отозвано. В связи с этим при передаче

13 CJEU, Schrems II, 2020, July 16, para. 65.

14 CJEU, Schrems II, 2020, July 16, paras. 91 and 92.

15 CJEU, Schrems II, 2020, July 16, para. 107 and case C-362/14, 2015, October 6, Schrems I, para. 47.

16 15 Эта точка зрения согласуется с выводами Суда по делу Schrems II от 2020 года и по делу Schrems I от 2015 года, а также с мнением таких ученых, как Piroddi (2021) и De Mozzi (2022).

17 CJEU, Schrems II, 2020, July 16, para. 120.

18 Этот принцип был применен в деле Schrems II от 2020 года.

19 CJEU, Schrems II, 2020, July 16, para. 168.

данных между США и ЕС должны применяться дополнительные меры безопасности, предусмотренные главой V Регламента ЕС, а именно статьей 46(2), в которой говорится о соответствующих гарантиях.

4 июня 2021 года Европейская комиссия утвердила два набора стандартных договорных соглашений в ответ на отмену Программы по защите конфиденциальности ЕС–США[20]. Цель этого решения – упростить передачу персональных данных из ЕС в третьи страны. Эти коммерческие соглашения отражают требования к передаче персональных данных в соответствии с решением Европейского суда по делу Schrems II, а также содержат положения, позволяющие учесть различное количество сторон, заключающих договор (De Mozzi, 2021).

3.3. Трансграничная передача данных внутри Евразийского экономического союза

Цифровые технологии открывают перед таможенными органами новые возможности для повышения скорости и качества процесса принятия решений. Следующий этап развития цифрового государственного управления тесно связан с централизацией данных. Это предполагает структурирование государственного управления, при котором решения все больше опираются на объективные данные (Vovchenko et al., 2019).

Еще один важный компонент цифровизации системы таможенного регулирования в ЕАЭС – это создание общей платформы для обмена и передачи цифровых данных, что подчеркивается в Положении о трансграничном пространстве доверия, а также в статье 23 соответствующего Соглашения.

Кроме того, Евразийская экономическая комиссия заложила основу для развития транснационального характера цифровой экономики. Это стало возможным благодаря решению Высшего Евразийского экономического совета № 12 от 11 октября 2017 года, утвердившему первоочередные планы реализации цифровой повестки ЕАЭС до 2025 г. (Колодняя, 2018).

Хотя большая часть вышеупомянутых законов была принята в рамках ЕАЭС, все еще имеется ряд барьеров, которые затрудняют плавное вхождение в союз всех его членов. Так, сохраняется проблема регулирования оборота данных на всей территории союза, представляя собой серьезное препятствие для реализации цифровой повестки. Многие цифровые экосистемы, планируемые к внедрению, предполагают трансграничный обмен данными в различных форматах взаимодействия, включая G2G, G2C, G2B, B 2B и B 2C. При этом многие аспекты обращения данных в ЕАЭС остаются недостаточно развитыми. Как следствие, отсутствует терминологическая согласованность ключевых понятий, связанных с данными, недостаточно развито регулирование в сфере данных, отсутствуют единые подходы к правовой категоризации данных и управлению рисками в этой сфере. Не решены правовые вопросы, связанные с трансграничным обменом данными. В результате нормативные меры отстают от практики, препятствуя прогрессу в реализации цифровой повестки. Ситуация еще более осложняется требованиями национальных законодательств государств-членов ЕАЭС, в частности, в области локализации персональных данных. Крайне важно создать и внедрить соответствующее законодательство и механизмы,

[20] Commission implementing decision of 4 June, Nos. 2021/914/UE and No. 2021/915/UE.

направленные на защиту данных при их трансграничном обращении внутри ЕАЭС, включая как неперсональные, так и персональные данные (Mikhaliova, 2022).

ЕАЭС давно участвует в дискуссиях о разработке международного соглашения, касающегося оборота и защиты данных. Однако процесс согласования подходов и разработки такого соглашения по-прежнему остается сложным и длительным.

Кроме того, сохраняются проблемы в сфере электронного документооборота. Следовательно, существует необходимость в совершенствовании законодательства и выработке общих подходов в области электронных подписей. Проблема взаимного признания электронных подписей является серьезным препятствием для торговли, существенно осложняя взаимодействие с поставщиками на внутреннем рынке ЕАЭС и процесс закупок. Эффективное использование цифровой инфраструктуры Союза невозможно без устранения этих правовых пробелов.

Еще более сложным препятствием на пути реализации цифровой повестки является проблема неравномерного развития цифровых технологий в государствах-членах Союза (Filatova et al., 2018). Чтобы продемонстрировать эту проблему, мы можем изучить показатели этих государств-членов в рамках Индекса сетевой готовности[21].

Индекс сетевой готовности был предложен в 2002 г. на Всемирном экономическом форуме и в настоящее время выпускается организацией Институт Портуланс (Portulans Institute). Индекс позволяет оценить степень развития информационно-коммуникационных технологий в разных странах. Он играет ключевую роль в оценке технологического и инновационного потенциала страны и является важным показателем для проведения сравнительных исследований в области ИКТ в разных государствах.

Что касается развития информационно-коммуникационных технологий в регионе ЕАЭС, то здесь наблюдается заметная диспропорция. Например, в 2022 г. разрыв в развитии ИКТ между Россией и Кыргызстаном составлял 45 пунктов. Армения, Беларусь и Казахстан достигли сопоставимого уровня развития ИКТ, но их отставание от России также значительно. В настоящее время основное внимание уделяется расширению связей между государственными органами государств-членов ЕАЭС, обновлению интегрированной информационной системы и внедрению безопасного и непрерывного электронного документооборота, что в определенной степени смягчает эту проблему.

Однако в будущем, когда цифровые инициативы Союза будут напрямую затрагивать интересы населения, это цифровое неравенство может существенно снизить эффективность реализации проектов. Кроме того, текущие цифровые инициативы опираются на уже существующие национальные сервисы, а разный уровень развития этих сервисов усложняет реализацию совместных проектов (Bolgov & Karachay, 2016). Чтобы ускорить цифровую трансформацию государств-членов ЕАЭС, необходимо активизировать международный обмен опытом в области цифровых технологий и распространение лучших технологических практик.

Важным фактором является то, что цифровая инфраструктура внутри Союза, в частности интегрированная информационная система, еще не полностью оформлена. Кроме того, задержки наблюдаются в реализации ряда важнейших проектов

[21] Network Readiness Index Homepage. https://networkreadinessindex.org

в рамках цифровой повестки. Основными препятствиями на пути развития цифровой экосистемы Союза являются недостатки нормативно-правовой базы, отсутствие последовательной концептуальной согласованности в реализации национальных стратегий развития цифровой экономики, а также диспропорции в развитии ИКТ в разных странах региона.

В последние годы государства ЕАЭС активно создают свои национальные цифровые экосистемы. Эти проекты охватывают как сферу государственного управления, так и цифровую экономику этих стран. Однако темп цифровизации в регионе отстает от развития национальных цифровых систем.

Для эффективной реализации целей и задач, которые задает цифровизация, необходимо консолидировать усилия государств ЕАЭС в области цифровой трансформации экономики. Такая консолидация предполагает более активное участие национальных центров компетенций и укрепление национальных цифровых инфраструктур.

Заключение

Очевидно, что в настоящее время международное сообщество как никогда нуждается в координированной нормативной базе, касающейся трансграничной передачи данных, включая правовые гарантии и меры для выявления уязвимостей в сфере безопасности, рисков кибербезопасности и правовых проблем.

Согласованные стандарты могут быть установлены лишь при условии достижения договоренностей по основным вопросам между ведущими державами и другими международными структурами. Предполагается, что эти нормы будут регулироваться не отдельными местными организациями, но образовывать обширный «режимный комплекс» под руководством «всеобщих» межправительственных органов. Как уже отмечалось, одним из ярких примеров гармонизированных стандартов является широкое распространение интернет-протокола TCP/IP.

Список литературы

Колодняя Г. (2018). Цифровая экономика: особенности развития в России. *Экономист*, *4*, 63–69.

Bennett, C. (2002). *United nations office for the coordination of humanitarian Affairs (UNOCHA) orientation handbook*.

Berleur, J. (2007). Governance Challenges: First Lessons from the WSIS – An Ethical and Social Perspective. In Ph. Goujon, S. Lavelle, P. Duquenoy, K. Kimppa, & V. Laurent (Eds.). *The Information Society*: *Innovation, Legitimacy, Ethics and Democracy In honor of Professor Jacques Berleur sj*: Proceedings of the Conference “Information Society: Governance, Ethics and Social Consequences”, University of Namur, Belgium 22–23 May 2006.

Bessette, R., & Haufler, V. (2001). Against All Odds: Why there is no International information regime. *International Studies Perspectives*, *2*(1), 69–92. https://doi.org/10.1111/1528-3577.00038

Bolgov, R., & Karachay, V. (2016). E-participation projects development in the E-governance institutional structure of the Eurasian Economic Union’s countries: comparative overview. In A. Chugunov, R. Bolgov, Y. Kabanov, G. Kampis, & M. Wimmer (Eds.), *Digital Transformation and Global Society: DTGS 2016. Communications in Computer and Information Science* (vol. 674). Springer, Cham. https://doi.org/10.1007/978-3-319-49700-6_20

Bruthans, J., & Jiráková, K. (2023). The Current State and Usage of European Electronic Cross-border Health Services (eHDSI). *Journal of Medical Systems*, *47*(1), 21. https://doi.org/10.1007/s10916-023-01920-9

Chuanying, L. (2020). Forging stability in cyberspace. *Survival*, *62*(2), 125–136. https://doi.org/10.1080/00396338.2020.1739959

De Moor, A., & Vermeulen, G. (2010). The Europol council decision: transforming Europol into an agency of the European Union. *Common Market Law Review*, *47*(4), 1089–1121. https://doi.org/10.54648/cola2010047

De Mozzi, B. (2021). Il ruolo delle Binding Corporate Rules: eteronomia e autonomia individuale nel diritto europeo ed extra-europeo. In *Privacy e lavoro. La circolazione dei dati personali ei controlli nel rapporto di lavoro* (pp. 140–161). Giuffrè Francis Lefebvre. (In Italy).

Drezner, D. W. (2004). The global governance of the Internet: Bringing the state back in. *Political Science Quarterly*, *119*(3), 477–498. https://doi.org/10.2307/20202392

Drezner, D. W. (2008). All politics is global: Explaining international regulatory regimes. Princeton University Press. https://doi.org/10.1515/9781400828630

Farrell, H. (2003). Constructing the international foundations of E-commerce – The EU-US Safe Harbor Arrangement. *International Organization*, *57*(2), 277–306. https://doi.org/10.1017/s0020818303572022

Filatova, O., Golubev, V., & Stetsko, E. (2018). Digital transformation in the Eurasian Economic Union: prospects and challenges. In D. Alexandrov, A. Boukhanovsky, A. Chugunov, Y. Kabanov, & O. Koltsova (Eds.), *Digital Transformation and Global Society. DTGS 2018. Communications in Computer and Information Science* (vol. 858). Springer, Cham. https://doi.org/10.1007/978-3-030-02843-5_8

Furramani, E. (2023). Transfer of Personal Data to Third Countries and the "Equivalent Level" of Protection According to the European Court of Justice. *European Journal of Formal Sciences and Engineering*, *6*(1), 1–12. https://doi.org/10.2478/ejfe-2023-0001

Gao, X., & Chen, X. (2022). Role enactment and the contestation of global cybersecurity governance. *Defence Studies*, *22*(4), 689–708. https://doi.org/10.1080/14702436.2022.2110485

Gurkov, A. (2021). Personal Data Protection in Russia. In D. Gritsenko, M. Wijermars, & M. Kopotev (Eds), *The Palgrave Handbook of Digital Russia Studies* (pp. 95–113). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-42855-6_6

Haufler, V. (2013). *A public role for the private sector: Industry self-regulation in a global economy*. Carnegie Endowment for International Peace. https://doi.org/10.2307/j.ctt6wpjtw

Hijmans, H. (2006). The European Data Protection Supervisor: The Institutions of the EC Controlled by an Independent Authority. *Common Market Law Review*, *43*(5), 1313–1342. https://doi.org/10.54648/cola2006076

Jensen, H. (2006). UN World Summit on the Information Society. In *Encyclopedia of Gender and Information Technology* (pp. 1172–1177). IGI Global. https://doi.org/10.4018/978-1-59140-815-4.ch185

Joel, A. (2023). A Trusted Framework for Cross-Border Data Flows. *Joint PIJIP/TLS Research Paper Series*, 114.

Long, W. J., & Quek, M. P. (2002). Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise. *Journal of European Public Policy*, *9*(3), 325–344. https://doi.org/10.1080/13501760210138778

Mai'a, K. (2023). *International Cooperation Against All Odds: The Ultrasocial World*. Oxford University Press.

Mikhaliova, T. N. (2022). Upgrading Legal Regulation of Integration in the Context of Digital Economy: The Eurasian Economic Union Agenda. In A. O. Inshakova, E. E. Frolova (Eds.), *Smart Technologies for the Digitisation of Industry: Entrepreneurial Environment. Smart Innovation, Systems and Technologies* (vol. 254, pp. 213–226). Springer, Singapore. https://doi.org/10.1007/978-981-16-4621-8_18

Nijboer, J. (2004). Big brother versus anonymity on the Internet: implications for Internet service providers, libraries and individuals since 9/11. *New Library World*, *105*(7/8), 256–261. https://doi.org/10.1108/03074800410551002

Niu, B., Xu, H., & Xie, F. (2021). Free shipping in cross-border supply chains considering tax disparity and carrier's pricing decisions. *Transportation Research Part E: Logistics and Transportation Review*, *152*, 102369. https://doi.org/10.1016/j.tre.2021.102369

Reidenberg, J. R. (1996). Governing networks and rule-making in cyberspace. *Emory Law Journal*, 45, 911. https://ir.lawnet.fordham.edu/faculty_scholarship/29

Press, L., Burkhart, G. E., Foster, W. A., Goodman, S. E., Wolcott, P., & Woodard, J. (1998). An Initial Inductive Study. *Communications of the ACM*, *41*(10), 21–26. https://doi.org/10.1145/286238.286242

Schneider, H. A. (2009). Katz v. United States: The Untold Story. *McGeorge Law Review*, *40*(1), 13. https://scholarlycommons.pacific.edu/mlr/vol40/iss1/2

Souter, D. (2004). The view from the summit: a report on the outcomes of the World Summit on the Information Society. *info*, *6*(1), 6–11. https://doi.org/10.1108/14636690410535881

Trump, B., Cummings, C., Klasa, K., Galaitsi, S., & Linkov, I. (2023). Governing biotechnology to provide safety and security and address ethical, legal, and social implications. *Frontiers in genetics*, *13*, 1052371. https://doi.org/10.3389/fgene.2022.1052371

Voss, W. G. (2019). Obstacles to transatlantic harmonization of data privacy law in context. U. Ill. JL Tech. & Pol'y, 405–463. https://ssrn.com/abstract=3446833

Vovchenko, N., Ivanova, O. B., Khapilin, A., & Khapilin, S. (2019). The Eurasian Economic Union customs' administration mechanism in the digital era. *International Journal of Economics and Business Administration*, *VII*(3), 133–139. https://doi.org/10.35808/ijeba/313

Информация об авторе

Болатбеккызы Гульбакыт – соискатель степени PhD, докторант, школа права, Уханьский университет
Адрес: 430072, Китай, провинция Хубэй, г. Ухань, Луоцзя Хилл
E-mail: gulbakyt@whu.edu.cn
ORCID ID: https://orcid.org/0009-0003-1990-1239
WoS Researcher ID: https://www.webofscience.com/wos/author/record/JEZ-7313–2023
Google Scholar ID: https://scholar.google.com/citations?user=RqrEh8YAAAAJ

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки.

Тематические рубрики

Рубрика OECD: 5.05 / Law
Рубрика ASJC: 3308 / Law
Рубрика WoS: OM / Law
Рубрика ГРНТИ: 10.19.61 / Правовое регулирование информационной безопасности
Специальность ВАК: 5.1.2 / Публично-правовые (государственно-правовые) науки

История статьи

Дата поступления – 2 февраля 2024 г.
Дата одобрения после рецензирования – 1 марта 2024 г.
Дата принятия к опубликованию – 25 июня 2024 г.
Дата онлайн-размещения – 30 июня 2024 г.

Research article
UDC 34:004:342.721:004.8
EDN: https://elibrary.ru/ppljhu
DOI: https://doi.org/10.21202/jdtl.2024.19

Legal Issues of Cross-Border Data Transfer in the Era of Digital Government

Gulbakyt Bolatbekkyzy
Wuhan University, Wuhan, China

Keywords

cybersecurity,
data protection,
digital government,
digital technologies,
digitalization,
human rights,
law,
personal data,
privacy,
transboundary exchange

Abstract

Objective: to identify the main legal factors of cross-border data exchange in the context of digital technology proliferation and government digitalization, including legal guarantees, security issues, cybersecurity risks, approaches to regulating and improving the efficiency of data management in various jurisdictions.

Methods: the study relies on synthesis and critical analysis of various aspects of the stated problem, including analysis of primary and secondary sources. By the example of the regulatory policies of China, the US, the EU and EAEU member states, different approaches regarding the restriction or encouragement of free cross-border data transfer are compared. A comprehensive meta-analysis and literature assessment provided insights into the methods used for data protection in different jurisdictions and allowed outlining the framework and directions of the public policy required for effective cross-jurisdictional data transfer.

Results: the main challenges associated with cross-border data transfer in the context of digital technology proliferation and government digitalization, such as growing inequalities in digital development, legal uncertainties, privacy and cybersecurity, etc., were identified. The legal framework of cross-border data transfer in the context of government digitalization and its implementation were analyzed. It contributed to the search for ways to improve the government efficiency in the context of transnational data transfer, including rendering services and promoting openness and public participation.

Scientific novelty: based on the analysis of various jurisdictions' approaches to legal, security and sovereignty issues caused by transnational data transfer, the author reveals the role and applicability of international law, as well as the unique challenges arising in the member states of the Eurasian Economic Union on the way to the formation of transboundary trust space.

Practical significance: the study of these issues may help various public agencies, first of all, governmental and legislative bodies to the elaborate well-targeted political and legal decisions, aimed at achieving a balance between data availability and data security, between the effectiveness of public administration and respect for the human rights. The results obtained will also be of importance for other subjects of relations in cross-border data transfer and regulation of these relations.

For citation

Bolatbekkyzy, G. (2024). Legal Issues of Cross-Border Data Transfer in the Era of Digital Government. *Journal of Digital Technologies and Law, 2*(2), 286–307. https://doi.org/10.21202/jdtl.2024.15

References

Bennett, C. (2002). *United nations office for the coordination of humanitarian Affairs (UNOCHA) orientation handbook*.

Berleur, J. (2007). Governance Challenges: First Lessons from the WSIS – An Ethical and Social Perspective. In Ph. Goujon, S. Lavelle, P. Duquenoy, K. Kimppa, & V. Laurent (Eds.). *The Information Society: Innovation, Legitimacy, Ethics and Democracy In honor of Professor Jacques Berleur sj*: Proceedings of the Conference "Information Society: Governance, Ethics and Social Consequences", University of Namur, Belgium 22–23 May 2006.

Bessette, R., & Haufler, V. (2001). Against All Odds: Why there is no International information regime. *International Studies Perspectives*, *2*(1), 69–92. https://doi.org/10.1111/1528-3577.00038

Bolgov, R., & Karachay, V. (2016). E-participation projects development in the E-governance institutional structure of the Eurasian Economic Union's countries: comparative overview. In A. Chugunov, R. Bolgov, Y. Kabanov, G. Kampis, & M. Wimmer (Eds.), *Digital Transformation and Global Society: DTGS 2016. Communications in Computer and Information Science* (vol. 674). Springer, Cham. https://doi.org/10.1007/978-3-319-49700-6_20

Bruthans, J., & Jiráková, K. (2023). The Current State and Usage of European Electronic Cross-border Health Services (eHDSI). *Journal of Medical Systems*, *47*(1), 21. https://doi.org/10.1007/s10916-023-01920-9

Chuanying, L. (2020). Forging stability in cyberspace. *Survival*, *62*(2), 125–136. https://doi.org/10.1080/00396338.2020.1739959

De Moor, A., & Vermeulen, G. (2010). The Europol council decision: transforming Europol into an agency of the European Union. *Common Market Law Review*, *47*(4), 1089–1121. https://doi.org/10.54648/cola2010047

De Mozzi, B. (2021). Il ruolo delle Binding Corporate Rules: eteronomia e autonomia individuale nel diritto europeo ed extra-europeo. In *Privacy e lavoro. La circolazione dei dati personali ei controlli nel rapporto di lavoro* (pp. 140–161). Giuffrè Francis Lefebvre. (In Italy).

Drezner, D. W. (2004). The global governance of the Internet: Bringing the state back in. *Political Science Quarterly*, *119*(3), 477–498. https://doi.org/10.2307/20202392

Drezner, D. W. (2008). All politics is global: Explaining international regulatory regimes. Princeton University Press. https://doi.org/10.1515/9781400828630

Farrell, H. (2003). Constructing the international foundations of E-commerce – The EU-US Safe Harbor Arrangement. *International Organization*, *57*(2), 277–306. https://doi.org/10.1017/s0020818303572022

Filatova, O., Golubev, V., & Stetsko, E. (2018). Digital transformation in the Eurasian Economic Union: prospects and challenges. In D. Alexandrov, A. Boukhanovsky, A. Chugunov, Y. Kabanov, & O. Koltsova (Eds.), *Digital Transformation and Global Society. DTGS 2018. Communications in Computer and Information Science* (vol. 858). Springer, Cham. https://doi.org/10.1007/978-3-030-02843-5_8

Furramani, E. (2023). Transfer of Personal Data to Third Countries and the "Equivalent Level" of Protection According to the European Court of Justice. *European Journal of Formal Sciences and Engineering*, *6*(1), 1–12. https://doi.org/10.2478/ejfe-2023-0001

Gao, X., & Chen, X. (2022). Role enactment and the contestation of global cybersecurity governance. *Defence Studies*, *22*(4), 689–708. https://doi.org/10.1080/14702436.2022.2110485

Gurkov, A. (2021). Personal Data Protection in Russia. In D. Gritsenko, M. Wijermars, & M. Kopotev (Eds), *The Palgrave Handbook of Digital Russia Studies* (pp. 95–113). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-030-42855-6_6

Haufler, V. (2013). *A public role for the private sector: Industry self-regulation in a global economy*. Carnegie Endowment for International Peace. https://doi.org/10.2307/j.ctt6wpjtw

Hijmans, H. (2006). The European Data Protection Supervisor: The Institutions of the EC Controlled by an Independent Authority. *Common Market Law Review*, *43*(5), 1313–1342. https://doi.org/10.54648/cola2006076

Jensen, H. (2006). UN World Summit on the Information Society. In *Encyclopedia of Gender and Information Technology* (pp. 1172–1177). IGI Global. https://doi.org/10.4018/978-1-59140-815-4.ch185

Joel, A. (2023). A Trusted Framework for Cross-Border Data Flows. *Joint PIJIP/TLS Research Paper Series*, 114.

Kolodnyaya, G. (2018). Digital economy: features of development in Russia. Ekonomist, 4, 63–69. (In Russ.).

Long, W. J., & Quek, M. P. (2002). Personal data privacy protection in an age of globalization: the US-EU safe harbor compromise. *Journal of European Public Policy*, *9*(3), 325–344. https://doi.org/10.1080/13501760210138778

Mai'a, K. (2023). *International Cooperation Against All Odds: The Ultrasocial World*. Oxford University Press.

Mikhaliova, T. N. (2022). Upgrading Legal Regulation of Integration in the Context of Digital Economy: The Eurasian Economic Union Agenda. In A. O. Inshakova, E. E. Frolova (Eds.), *Smart Technologies for the Digitisation of Industry: Entrepreneurial Environment. Smart Innovation, Systems and Technologies* (vol. 254, pp. 213–226). Springer, Singapore. https://doi.org/10.1007/978-981-16-4621-8_18

Nijboer, J. (2004). Big brother versus anonymity on the Internet: implications for Internet service providers, libraries and individuals since 9/11. *New Library World*, *105*(7/8), 256–261. https://doi.org/10.1108/03074800410551002

Niu, B., Xu, H., & Xie, F. (2021). Free shipping in cross-border supply chains considering tax disparity and carrier's pricing decisions. *Transportation Research Part E: Logistics and Transportation Review*, *152*, 102369. https://doi.org/10.1016/j.tre.2021.102369

Reidenberg, J. R. (1996). Governing networks and rule-making in cyberspace. *Emory Law Journal*, 45, 911. https://ir.lawnet.fordham.edu/faculty_scholarship/29

Press, L., Burkhart, G. E., Foster, W. A., Goodman, S. E., Wolcott, P., & Woodard, J. (1998). An Initial Inductive Study. *Communications of the ACM*, *41*(10), 21–26. https://doi.org/10.1145/286238.286242

Schneider, H. A. (2009). Katz v. United States: The Untold Story. *McGeorge Law Review*, *40*(1), 13. https://scholarlycommons.pacific.edu/mlr/vol40/iss1/2

Souter, D. (2004). The view from the summit: a report on the outcomes of the World Summit on the Information Society. *info*, *6*(1), 6–11. https://doi.org/10.1108/14636690410535881

Trump, B., Cummings, C., Klasa, K., Galaitsi, S., & Linkov, I. (2023). Governing biotechnology to provide safety and security and address ethical, legal, and social implications. *Frontiers in genetics*, *13*, 1052371. https://doi.org/10.3389/fgene.2022.1052371

Voss, W. G. (2019). Obstacles to transatlantic harmonization of data privacy law in context. U. Ill. JL Tech. & Pol'y, 405–463. https://ssrn.com/abstract=3446833

Vovchenko, N., Ivanova, O. B., Khapilin, A., & Khapilin, S. (2019). The Eurasian Economic Union customs' administration mechanism in the digital era. *International Journal of Economics and Business Administration*, *VII*(3), 133–139. https://doi.org/10.35808/ijeba/313

Author information

Gulbakyt Bolatbekkyzy – PhD Candidate and Doctoral Scholar, School of Law, Wuhan University
Address: Luojia Hill, Wuhan, Hubei Province, 430072, China
E-mail: gulbakyt@whu.edu.cn
ORCID ID: https://orcid.org/0009-0003-1990-1239
WoS Researcher ID: https://www.webofscience.com/wos/author/record/JEZ-7313-2023
Google Scholar ID: https://scholar.google.com/citations?user=RqrEh8YAAAAJ

Conflicts of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law
PASJC: 3308 / Law
WoS: OM / Law

Article history

Date of receipt – February 2, 2024
Date of approval – March 1, 2024
Date of acceptance – June 25, 2024
Date of online placement – June 30, 2024