

Дата поступления рукописи в редакцию: 20.01.2026 г.
Дата принятия рукописи в печать: 16.02.2026 г.

DOI: 10.24412/2076-1503-2026-1-279-288

ГОЛУБЦОВА Оксана Анатольевна,
кандидат экономических наук, доцент,
ORCID 0000-0003-2428-3642,
e-mail: gragov777@mail.ru

МОДЕЛИ ПРАВОВОГО РЕГУЛИРОВАНИЯ ТРАНСГРАНИЧНЫХ ПОТОКОВ ДАННЫХ В КОНТЕКСТЕ ЦИФРОВОЙ ЭКОНОМИКИ

Аннотация. Данная статья посвящена анализу сложной и динамично развивающейся правовой среды, регулирующей трансграничные потоки данных (ТПД) в контексте глобальной цифровой экономики. Отмечается, что, несмотря на критическую роль ТПД в международной торговле, их перемещение сталкивается с растущими ограничениями, обусловленными конкуренцией стандартов и экстерриториальным применением законодательства, что приводит к ужесточению требований локализации данных. Исследование рассматривает ключевые аспекты правового регулирования, включая защиту персональных данных (на примере GDPR), безопасность, прозрачность и ответственность. Выделяются три основных подхода к контролю ТПД: полный запрет, ограничения (например, необходимость получения разрешений или соответствия «адекватному» уровню защиты) и наличие исключений. Проводится компаративный анализ четырех типологических моделей регулирования ТПД: либеральной (США, Сингапур), условной (ЕС, Япония), ограничительной/локализационной (Китай, РФ) и гибридной. Анализ опыта Азии показывает, как регуляторы стимулируют развитие цифровых экосистем через стандартизацию (SGFinDex) или государственно-рыночный симбиоз (China BigTech). Особое внимание уделено политике либерализации, закреплённой в таких соглашениях, как CPTPP и USMCA, и ее положительному экономическому влиянию (повышение объемов цифровой торговли, снижение издержек). Однако либерализация сталкивается с серьезными препятствиями, в частности, с конфликтом конституционных основ защиты прав, ярко проиллюстрированным серией судебных дел Schrems (ЕС против США). Этот конфликт между фундаментальным правом на конфиденциальность в ЕС и требованиями национальной безопасности в США создает хроническую правовую неопределенность. Для оценки регуляторного давления используется методология Индекса ограничений цифровой торговли (DTRI) от ECIPE, которая выявляет значительную внутреннюю гетерогенность даже в рамках условной модели ЕС, где ключевые страны (Германия, Франция) применяют более жесткие меры. Доминирующей тенденцией является усиление государственного контроля над ТПД. Регуляторные различия, особенно между либеральными и локализационными режимами, формируют фрагментированную глобальную архитектуру, которая препятствует полной гармонизации цифровой торговли.

Ключевые слова: трансграничные потоки данных, регулирование, модель, цифровая экономика, международная торговля, законодательство о защите данных.

GOLUBTSOVA Oksana Anatolyevna,
Candidate of economic sciences, associate professor,
ORCID 0000-0003-2428-3642

MODELS OF LEGAL REGULATION OF CROSS-BORDER DATA FLOWS IN THE CONTEXT OF THE DIGITAL ECONOMY

Annotation. This article is dedicated to analyzing the complex and dynamically evolving legal environment governing Cross-Border Data Flows (CBDF) within the global digital economy. It is noted that, despite the critical role of CBDF in international trade, their movement faces growing restrictions stemming from competing standards and the extraterritorial application of legislation, leading to stricter data localization requirements. The study examines key aspects of legal regulation, including

personal data protection (using the GDPR as an example), security, transparency, and accountability. Three main approaches to controlling CBDF are highlighted: outright prohibition, restrictions (such as the need to obtain permits or conform to an “adequate” level of protection), and the existence of exceptions. A comparative analysis is conducted on four typological models of CBDF regulation: the liberal model (US, Singapore), the conditional model (EU, Japan), the restrictive/localization model (China, RF), and the hybrid model. An analysis of the Asian experience demonstrates how regulators stimulate the development of digital ecosystems through standardization (SGFinDex) or a state-market symbiosis (China BigTech). Special attention is paid to liberalization policies enshrined in agreements like CPTPP and USMCA, and their positive economic impact (increased digital trade volumes, reduced costs). However, liberalization confronts significant obstacles, particularly the conflict between constitutional foundations of rights protection, vividly illustrated by the Schrems case series (EU vs. US). This conflict between the fundamental right to privacy in the EU and national security requirements in the US creates chronic legal uncertainty. To assess regulatory pressure, the methodology of the Digital Trade Restriction Index (DTRI) from ECIPE is employed. This reveals significant internal heterogeneity even within the EU’s conditional model, where key countries (Germany, France) apply stricter measures. The dominant trend is the intensification of state control over CBDF. Regulatory divergences, especially between liberal and localization regimes, form a fragmented global architecture that hinders the full harmonization of digital trade.

Key words: cross-border data flows, regulation, model, digital economy, international trade, data protection legislation.

Введение

Современный этап развития мировой экономики характеризуется стремительным распространением цифровых технологий, активно трансформирующих финансовую систему, изменяя как ее инструменты, так и механизмы регулирования. Цифровая трансформация включает различные аспекты – от электронных платежных систем и цифровой идентификации до использования блокчейн-технологий, искусственного интеллекта и финансовых технологий. Цифровизация экономики привела к беспрецедентному росту трансграничных потоков данных, которые являются ценным экономическим активом. Это порождает сложные правовые вопросы, касающиеся суверенитета над данными, защиты конфиденциальности, предотвращения дискриминации по месту происхождения данных, а также регулирования доступа к данным для целей экономического развития и обеспечения конкуренции. Отсутствие единых международных стандартов создает правовую неопределенность и потенциальные барьеры для международной торговли и инвестиций.

Такое динамичное развитие требует соответствующего правового обеспечения, гарантирующего эффективность и безопасность функционирования трансграничных потоков данных.

Цель статьи – исследование моделей правового регулирования трансграничных потоков данных в контексте цифровой экономики.

Задачи исследования:

- рассмотреть основные аспекты правового регулирования трансграничных потоков данных;

- исследовать основные подходы к контролю трансграничных потоков данных;
- провести анализ типологических моделей регулирования трансграничных потоков данных;
- оценить влияние регулирования трансграничных потоков данных на существующие ограничения цифровой торговли.

Материалы и методы

Исследование основано на смешанном подходе, сочетающем доктринальный юридический анализ с компаративным обзором политики. Основными материалами послужил анализ нормативно-правовой базы, регулирующей трансграничные потоки данных. Кроме того, исследование включает сравнительный обзор конкретных положений, касающихся электронной коммерции и трансграничных потоков данных (ТПД), зафиксированных в преференциальных соглашениях. Для обеспечения всестороннего понимания развивающейся терминологической базы были использованы вторичные данные: аналитические материалы и экспертные публикации международных организаций.

Трансграничные потоки данных, будучи неотъемлемой частью международной торговли и фундаментом для множества цифровых сервисов, сталкиваются с растущими ограничениями. Это обусловлено сосуществованием конкурирующих стандартов и экстерриториальным применением законодательства, что приводит к ужесточению требований к локализации данных и ограничению их международной передачи [1, с. 58].

Правовое регулирование трансграничных потоков данных в контексте цифровой экономики

включает национальное законодательство, международные соглашения и рекомендации международных организаций. Цель – обеспечить защиту конфиденциальности и безопасности данных при трансграничной передаче, при этом, не препятствуя развитию цифровой экономики. Основными аспектами правового регулирования трансграничных потоков данных являются:

Во-первых, защита персональных данных, в частности законодательство, такое как Общий регламент о защите данных (GDPR), устанавливает строгие правила сбора, обработки и передачи персональных данных граждан Европейского Союза, даже если данные передаются за пределы ЕС. Это включает требования к согласию субъекта данных, прав на доступ, исправление и удаление данных [2].

Во-вторых, трансграничная передача данных, поскольку регулирование определяет условия, при которых персональные данные могут быть переданы странам, не имеющим аналогичного уровня защиты данных. Это может включать в себя использование стандартных договорных положений (Standard Contractual Clauses) или других механизмов, обеспечивающих надлежащую защиту данных [3, с. 83].

В-третьих, безопасность и конфиденциальность. Законодательство требует осуществлять соответствующие технические и организационные меры по защите данных от несанкционированного доступа, потери или кражи.

В-четвертых, прозрачность. Компании должны четко информировать пользователей о том, какие данные собираются, как они используются и с кем они передаются.

И, в-пятых, ответственность. Определяется ответственность субъектов, обрабатывающих данные (контролеры и обработчики) за соблюдение законодательства и принятие мер по защите данных [4, с. 56].

В практике уже сформировались определенные подходы к регулированию трансграничной передачи персональных и других категорий «чувствительных» данных, в частности, можно выделить следующие:

- первый, это полный запрет на передачу данных – применяется лишь небольшим числом стран. Например, в Саудовской Аравии конфиденциальные данные государственных органов и потребительские данные частных фирм не могут передаваться за пределы страны [5, с. 161];
- второй, ограничения на трансграничную передачу – могут быть связаны с необходимостью получения разрешения ответственных органов власти или согласия субъекта персональных данных, например в ЕС дей-

ствуют ограничения на трансграничную передачу персональных данных (регламент GDPR) [2]. В отдельных случаях передача данных возможна лишь в страны с «адекватным» уровнем защиты;

- третий, исключения, в частности во многих странах существует обширный список исключений, обеспечивающих свободу передачи данных, например, согласно условиям контракта или в случае обеспечения жизненно важных интересов субъекта персональных данных при невозможности получения его согласия.

Трансграничные потоки данных сегодня являются важным компонентом международной торговли и основой многих моделей цифровых услуг. Однако по разным причинам в условиях «конкурирующих стандартов» и «пересечения норм» экстерриториальных законов усилились ограничения на передачу персональных данных и требования по локализации данных.

Результаты и обсуждение

Рассматривавшая мировую практику можно выделить опыт Азии, которая выступает в роли динамичного полигона для разработки и внедрения инновационных моделей цифровых финансовых экосистем, с акцентом на развитие концепций «open banking» и «open finance». Анализ кейсов Китая, Сингапура и Индии позволяет сформулировать следующие ключевые выводы, касающиеся следующего: во-первых, в Китае наблюдается симбиоз рыночных сил (BigTech-платформ) и регуляторного вмешательства. Изначально созданные частными компаниями суперапы стали катализатором для внедрения «open finance», а последующие действия регулятора (ПБОС) институционализировали этот процесс, обеспечив государственный контроль и стандартизацию [6, с. 55]; во-вторых, децентрализованные и централизованные подходы, в частности Сингапур представляет модель, где регулятор (MAS) активно формирует среду для «open banking» посредством стандартизации (API Playbook), создания платформ для взаимодействия (APIX) и интеграции данных (SGFinDex) [5, с. 165]. Индия, напротив, демонстрирует архитектуру, основанную на унифицированной государственной цифровой инфраструктуре (India Stack) и специализированных лицензированных посредниках (Account Aggregator), что обеспечивает децентрализованное, но контролируемое движение данных [5, с. 165].

Таким образом, регуляторы играют критически важную роль в формировании правовой базы, стандартов безопасности, а также в обеспечении прозрачности и защиты прав потребителей. Их

действия либо напрямую стимулируют развитие (Сингапур, Индия), либо институционализируют уже существующие рыночные тренды (Китай).

В России принят Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» от 21.07.2014 № 242-ФЗ, требующий, чтобы все базы, в которых хранятся персональные данные российских граждан, физически находились в России. Он предусматривает следующее. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети «Интернет», оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, указанных в пунктах 2, 3, 4, 8 части 1 статьи 6.

Политика регулирования трансграничных потоков данных играет ключевую роль в цифровой торговле и определяет всеобщий вектор ее регулирования в отдельных странах мира. Для регулирования трансграничных потоков данных используются два вида политик: политика либерализации и политика локализации движения трансграничных потоков данных.

Политика либерализации трансграничных потоков данных – это совокупность регуляторных и политических мер, направленных на содействие свободному, безопасному и неограниченному перемещению данных через государственные границы в контексте цифровой экономики [8, с. 23]. Целями политики либерализации трансграничных потоков данных являются:

- обеспечение бесперебойного обмена данными для поддержки электронной коммерции, облачных вычислений, искусственного интеллекта и других цифровых технологий;
- уменьшение затрат для компаний, особенно МСП, путем устранения необходимости создавать локальные центры данных;
- предоставление доступа к глобальным данным для развития технологий, таких как ИИ, зависящие от больших объемов информации;
- содействие гармонизации стандартов для обеспечения совместимости цифровых систем между странами.

Следовательно, политика либерализации трансграничных потоков данных достигает своих целей путем уменьшения барьеров, таких как требования локализации данных для облегчения электронной коммерции, цифровых услуг и гло-

бальных цепей поставок, обеспечивая при этом защиту конфиденциальности, кибербезопасность и соответствие национальным интересам. Она является ключевым элементом цифровой торговой политики, способствующей экономическому росту, инновациям и глобальной интеграции.

Можно выделить следующие основные инструменты политики либерализации трансграничных потоков данных:

- запрет локализации данных в региональных торговых соглашениях. В частности, Всеобъемлющее и прогрессивное соглашение о Транстихоокеанском партнерстве (СРТПП) запрещает требования хранить данные исключительно в пределах страны (статья 14.13) [10]. Подписантами Соглашения являются Австралия, Бруней, Канада, Чили, Япония, Малайзия, Мексика, Перу, Новая Зеландия, Сингапур и Вьетнам. Настоящее Соглашение является первым многосторонним соглашением, специально рассматривающим экономические и торговые вопросы, связанные с Интернетом, и включает в себя новаторские положения относительно онлайн-конфиденциальности, кибербезопасности, содействия трансграничным потокам данных и политики конкуренции. При этом СРТПП поддерживает более широкое использование ИКТ в экономике региона с целью преодоления вызовов цифрового разрыва [9]. Соглашение USMCA также запрещает ограничения на трансграничные потоки данных для коммерческих целей, за исключением законных соображений безопасности (статья 19.11);
- мораторий на таможенные пошлины. Декларация по глобальной электронной коммерции ВТО, принятая в 1998 г., содержит так называемый мораторий на использование таможенных пошлин в электронной коммерции;
- стандарты защиты данных. Установление минимальных стандартов защиты данных, позволяющих передачу данных в страны с соответствующим уровнем защиты (например, Общий регламент о защите данных (General Data Protection Regulation, GDPR)) ЕС, устанавливающий правила по защите персональных данных физических лиц [2];
- международные соглашения по цифровой экономике (Digital Economy Agreements (DEAs)). Целью соглашения о цифровой экономике является создание и установка международных правил, способствующих цифровой торговле, а также облегчение взаимодействия путем согласования стандартов, способствующие свободному движению

данных. Примерами международных соглашений в области цифровой экономики являются Инициатива совместного заявления по электронной коммерции ВТО (The Joint Statement Initiative (JSI)²¹) и Соглашение о партнерстве в области цифровой экономики (Digital Economy Partnership Agreement (DEPA)).

В июле 2024 года Сингапур, Австралия и Япония как соорганизаторы JSI объявили, что участники достигли договоренности, что стало важной вехой после пяти лет переговоров. По состоянию на 25 июня 2024 г. в этих обсуждениях принимает участие 91 член ВТО.

DEPA – это первое соглашение, которое устанавливает новые подходы и сотрудничество в вопросах цифровой торговли, способствует взаимодействию между разными режимами данных и решает новые проблемы цифровых технологий [9]. DEPA была подписана в июне 2020 г. между Сингапуром, Чили и Новой Зеландией. Соглашение устанавливает правила для свободного движения данных, включая положения о доверии к цифровым системам и кибербезопасности. В мае 2024 к соглашению присоединилась Республика Корея и семь стран-претендентов подали заявки на присоединение к DEPA, это Китай, Канада, Коста-Рика, Перу, Соединенные Арабские Эмираты (ОАЭ), Сальвадор.

Анализ влияния политики либерализации трансграничных потоков данных на цифровую торговлю показал, что либерализация трансграничных потоков данных приводит к следующим положительным эффектам:

- либерализация трансграничных потоков данных уменьшает административные и логистические расходы благодаря автоматизации процессов таможенного оформления через блокчейн и электронные документы;
- по оценкам OECD, либерализация трансграничных потоков данных может увеличить объемы цифровой торговли на 2-4% в секторах, зависимых от данных, таких как программное обеспечение, облачные вычисления;
- МСП получают возможность конкурировать на глобальном уровне, используя цифровые платформы;
- свободный доступ к данным способствует развитию ИИ, аналитики обширных данных и финтех;
- по оценкам ВТО, либерализация цифровой торговли может добавить в глобальный ВВП 0,1-0,3% ежегодно за счет повышения производительности, внедрения инноваций и снижения барьеров доступа к рынкам;

- по оценкам OECD, либерализация потоков данных может удвоить экономические выгоды от торговых сделок. МВФ подчеркивает, что поддержка открытых потоков данных оказывает минимальное влияние на потерю таможенных доходов (0,01-0,33% доходов правительств), но значительно способствует экономической эффективности [12].

Вместе с тем, либерализация трансграничных потоков данных создает определенные вызовы, а сам процесс либерализации сталкивается с определенными препятствиями. Препятствия на пути к полной либерализации трансграничных потоков данных носят многоуровневый характер и коренятся в конфликте приоритетов между экономическими интересами и суверенными требованиями.

Фрагментация регуляторной среды является центральным препятствием для формирования единого глобального цифрового рынка. Этот феномен проявляется в несогласованности законодательных режимов, что фактически ингибирует беспрепятственное перемещение информации.

Одним из наиболее значимых барьеров выступает институционализированный принцип эквивалентности, применяемый в условных моделях регулирования, в частности, в Европейском Союзе. GDPR устанавливает, что передача персональных данных за пределы юрисдикции ЕС допустима только в те юрисдикции, которые обеспечивают сопоставимый (адекватный) уровень правовой защиты [2].

Правовая неопределенность, порожденная этим требованием, была усугублена прецедентным правом Европейского Суда (ЕСС), в частности решением по делу Schrems II (Июль 2020 г.). Данное постановление дезактивировало механизм Privacy Shield, который регулировал трансфер данных между ЕС и США. Это решение не только поставило под сомнение легитимность массовой передачи данных в США, но и ввело дополнительные операционные требования ко всем трансферам в юрисдикции, не обладающие формальным признаком адекватности [14]. Это фактически повысило транзакционные издержки для трансграничных операций, требуя от субъектов имплементации дополнительных гарантий (например, SCCs).

Проблема достижения оптимального регуляторного баланса при трансграничной передаче данных наиболее наглядно демонстрируется эволюцией судебной практики в отношениях между Соединенными Штатами Америки и Европейским Союзом. Данный тандем юрисдикций, представ-

ляющий собой, с одной стороны, либерально-ориентированную модель (США), а с другой — условно-сбалансированную (ЕС), служит эмпирическим полигоном для анализа фундаментальных импедиментов гармонизации в сфере защиты персональных данных.

Серия судебных разбирательств, известная как дела Schrems, служит мощным прецедентным маркером, иллюстрирующим неспособность даже формализованных двусторонних соглашений по трансферу данных обеспечить стабильное и оптимальное равновесие интересов сторон.

Последовательные решения Европейского Суда (ЕСС) в рамках этой серии дел выявили глубокую методологическую и конституционную несовместимость подходов к защите прав субъектов данных в двух юрисдикциях:

Дело Schrems I (2015) привело к аннулированию Рамочного соглашения Safe Harbour. Это решение акцентировало внимание на рисках, связанных с доступом государственных органов США к переданным данным, что было признано несовместимым с принципом соразмерности, закрепленным в Хартии ЕС об основных правах.

Дело Schrems II (2020) послужило более радикальным шагом, аннулируя механизм Privacy Shield. Решение закрепило жесткое требование экстерриториальной эквивалентности защиты данных. ЕСС постановил, что сам по себе закон США, предоставляющий государственным органам широкие возможности доступа к данным граждан ЕС, девальвирует уровень защиты, обеспечиваемый GDPR.

Дело Schrems III (потенциальное развитие) продолжение дискуссий (в частности, относительно нового механизма Data Privacy Framework) свидетельствует о персистентном характере конфликта, который не может быть полностью урегулирован на уровне межправительственных соглашений без структурной реформы законодательства о доступе к данным в юрисдикции-реципиенте (США).

Эволюция Schrems демонстрирует, что основные препятствия к гармонизации лежат не в технической или торговой плоскости, а в конституционно-правовой доктрине двух регионов. Во-первых, концептуальный разрыв в понимании неприкосновенности частной жизни. В ЕС права на конфиденциальность рассматриваются как абсолютные фундаментальные права, требующие защиты от избыточного государственного вмешательства. В США доминирует подход, который, хотя и признает конфиденциальность, часто подчиняет ее требованиям национальной безопасности и правоохранительной деятельности. Во-вторых, проблема имплементации экстерриториальных стан-

дартов. ЕС обязывает компании применять стандарты GDPR ко всем передаваемым данным, независимо от местоположения конечного получателя. США, в свою очередь, обладают внутренним законодательством, которое зачастую вступает в конфликт с этими экстерриториальными требованиями, ставя операторов в неразрешимую дилемму (legal trap).

Таким образом, опыт США и ЕС доказывает, что либерализация трансграничной передачи данных в условиях диаметрально противоположных конституционных основ защиты прав граждан неизбежно ведет к правовой нестабильности и регуляторным кризисам, которые могут быть разрешены только через глубокую реформу одной из сторон или создание беспрецедентно сильных механизмов пересмотра двусторонних договоров.

Анализ судебной траектории Schrems I, II (и потенциала Schrems III) позволяет сделать вывод о том, что конфликт между регуляторными режимами США и ЕС в области трансграничной передачи данных является фундаментальным и структурным, а не поверхностным.

Либерализация трансграничных потоков данных вступает в прямое противоречие с императивами национальной кибербезопасности и цифрового суверенитета. Ряд государств (включая Китай и Российскую Федерацию) применяют стратегию цифрового протекционизма, ограничивая исходящие потоки данных. Такая политика обусловлена необходимостью обеспечения государственного контроля над критически важной информацией и персональными данными граждан. Данный протекционизм, хотя и легитимен с точки зрения национального права, структурно препятствует достижению глобальной гармонизации и либерализации цифровой торговли, создавая дихотомию между открытыми и закрытыми юрисдикция-ми.

Более того, сама по себе либерализация цифровой торговли (в смысле устранения тарифных барьеров) может усугублять феномен цифрового неравенства. Страны, не обладающие развитой цифровой инфраструктурой и высококвалифицированными кадрами, могут оказаться неспособными эффективно интегрироваться в либерализованные потоки, что приводит к углублению разрыва между технологически развитыми и развивающимися экономиками.

Политика локализации трансграничных потоков данных (data localization policies) предусматривает требования, согласно которым данные, собранные в одной стране, должны храниться, обрабатываться или оставаться в пределах ее юрисдикции. Политика локализации данных требует, чтобы компании хранили данные на серверах

рах внутри страны, где они были собраны, или ограничивает их передачу за границу. Соответствующие политики регулируются нормами законов о защите персональных данных, требованиях к локальным серверам или об ограничениях на трансграничное движение данных. Например, в Китае политика локализации трансграничных потоков данных регулируется Законом о кибербезопасности (2017), нормы которого требуют хранения «критических данных» в пределах страны, что способствует развитию местных компаний, таких как Alibaba, но ограничивает доступ иностранных компаний, снижая их конкурентоспособность [15].

Целью политики локализации трансграничных потоков данных является национальная и кибербезопасность, обеспечение конфиденциальности данных граждан, стимулирование развития местной цифровой инфраструктуры, контроль над экономическими выгодами от данных.

По результатам исследования научных публикаций [9, 11] и публикаций международных организаций можно выделить подходы к регулированию трансграничных потоков данных систематизированные в четыре типологические модели, отражающие сложный компромисс между стимулированием цифровой экономики, обеспечением конфиденциальности персональных данных и требованиями национальной кибербезопасности. Идентификация моделей осуществляется на основе анализа степени вмешательства государства в процесс передачи информации за юрисдикционные пределы.

Либеральная (открытая) модель характеризуется минимальным уровнем регуляторного вмешательства, что максимизирует экономический потенциал цифровой торговли. Данный подход доминирует в юрисдикциях, ориентированных на стимулирование инноваций, таких как США и Сингапур. Однако эта модель имплицитно сопряжена с повышенными рисками в сфере защиты субъективных прав на конфиденциальность.

Условная (сбалансированная) модель представляет собой регуляторный гибрид, нацеленный на синтез принципов свободной торговли и адекватной защиты данных. Наиболее ярким примером выступает Европейский Союз (ЕС) и Япония. Регулирование здесь усложнено необходимостью соблюдения условий эквивалентности (принцип «должного уровня защиты»).

В основе ограничительной (закрытой) модели приоритет обеспечения суверенитета и национальной безопасности. Для таких юрисдикций, как Китайская Народная Республика и Российская Федерация, характерен жесткий локали-

зационный режим, требующий обязательного хранения данных в пределах национальной территории, что создает существенные барьеры для транснациональных цифровых операций.

Гибридная (компромиссная) модель применяется странами, находящимися на этапе ускоренного цифрового развития (Бразилия, Южная Корея). Она характеризуется стремлением к сбалансированности, однако ее реализация часто требует значительных капиталовложений в национальную цифровую инфраструктуру.

Для эмпирического исследования и сопоставления данных моделей исследователи применяют многофакторные методологии, основанные на компаративном анализе, из которых можно выделить следующие:

- анализ международных соглашений, включающий в себя оценку положений, касающихся цифровой торговли, в рамках многосторонних и двусторонних соглашений (например, DEPA, CPTPP, RCEP) [11].
- таксономия ограничений (ECIPE) методология, разработанная Европейским центром международной политической экономики (ECIPE) [16], фокусируется на классификации регуляторных мер по их степени строгости: строгие ограничения (требование локального хранения) и условные ограничения (передача данных при соблюдении условий, как в GDPR). Согласно методологии ECIPE, ограничения на трансграничные потоки данных классифицируют как «строгие», когда они специально требуют хранения данных локально, или как «условные», когда они устанавливают определенные условия для передачи данных через границу.

Европейский режим защиты данных GDPR является обычным примером условного режима. Согласно законодательству ЕС условия применяются как к стране-получателю, так и к субъекту, передающему данные. В первом случае компания может передавать данные за границу странам с «должным уровнем защиты». Во втором случае, даже если страна-получатель не считается имеющей «должный уровень защиты», данные могут быть переданы и обрабатываться за границей, если получатель отвечает определенным условиям.

Индекс DTRI (Digital Trade Restriction Index), разработанный ECIPE, является количественным инструментом, оценивающим регуляторное давление через анализ более ста категорий политик в 64 юрисдикциях. Анализ DTRI выявляет внутрирегиональную гетерогенность даже в рамках условной модели (ЕС).

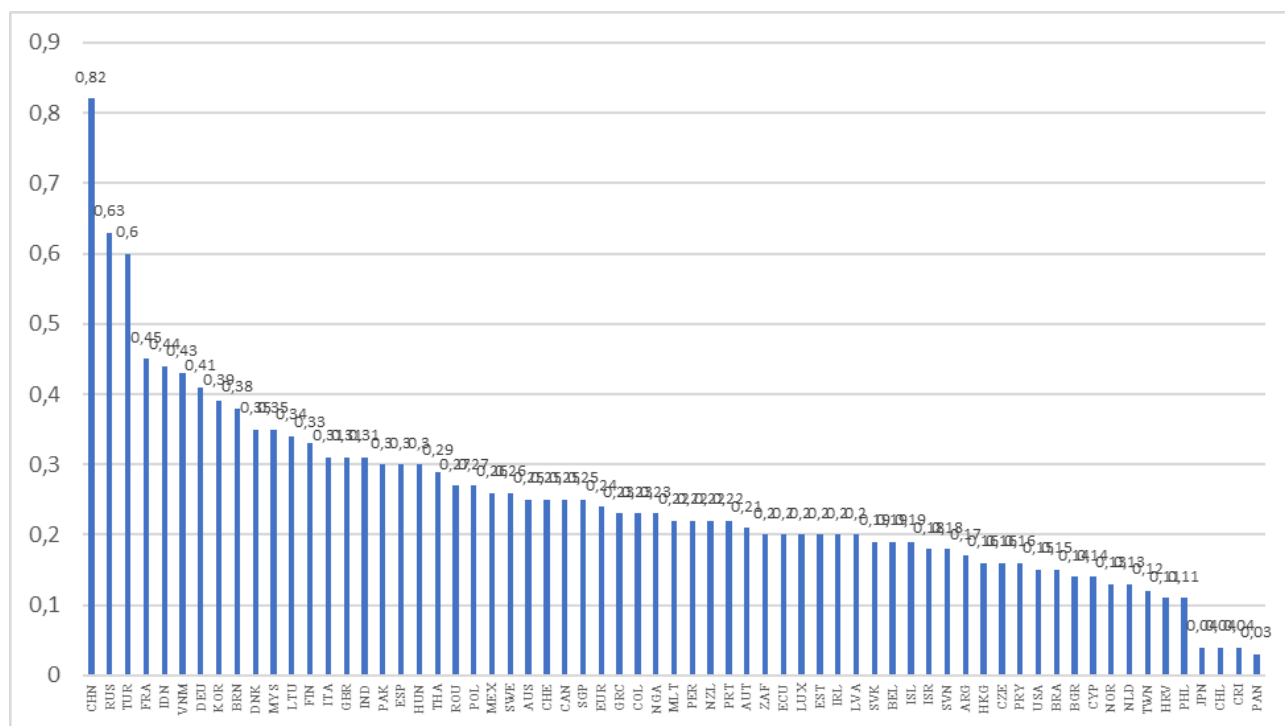


Рисунок 1. Индекс DTRI

Общий агрегированный рейтинг ЕС в индексе DTRI помещает его на средние позиции (21-е место). Однако отдельные государства-члены демонстрируют значительно более жесткие режимы. Например, Германия (13-е место), Франция (9-е место), и ряд стран Северной Европы (Дания, Финляндия) занимают топовые позиции по жесткости ограничений ТПД, превышая средний уровень ЕС.

Критическим наблюдением является наличие жестких локализационных мер, разрешающих правительственный доступ к корпоративным данным без санкции суда, что характерно для Франции и сопоставимо по строгости с режимами Китая, РФ, Турции и Вьетнама. И наоборот, наименьшие ограничения в ЕС наблюдаются в юрисдикциях с высокоразвитым сектором услуг (Ирландия, Мальта, Нидерланды).

Таким образом, анализ парадигм регулирования трансграничных потоков данных демонстрирует, что глобальная регуляторная архитектура не является унифицированной, а представляет собой сочетание из четырех фундаментальных моделей (либеральная, условная, ограничительная, гибридная), каждая из которых устанавливает различный баланс между экономическими стимулами и защитой суверенных/конфиденциальных интересов.

Заключение

В результате проведенного исследования можно сделать ключевые методологические и эмпирические заключения. Оценка регуляторного давления базируется на компаративных методологиях, в частности, таксономии ECIPE (DTRI), которая позволяет количественно измерить строгость ограничений, включая требование локализации данных. Европейский подход, несмотря на статус GDPR как эталона условного регулирования, демонстрирует значительную внутреннюю гетерогенность. Ряд ключевых стран-членов ЕС (Франция, Германия) проводят более жесткую политику, приближаясь по уровню некоторых ограничений к ограничительной модели, что говорит о неоднородности условной модели.

Прецедентная практика ЕСС показала, что дипломатически согласованные механизмы (как Privacy Shield) не обладают достаточной устойчивостью при столкновении с незыблемыми конституционными ценностями, особенно в части ограничения государственного доступа к данным. Корень проблемы лежит в различном иерархическом положении права на конфиденциальность относительно интересов национальной безопасности в правовых системах США и ЕС. Отмена ключевых механизмов трансфера данных создает хроническую неопределенность для бизнеса,

вынуждая операторов данных действовать в условиях постоянного риска правовой нелегитимности их транзакций, что тормозит полную либерализацию цифровой торговли между этими крупнейшими экономическими блоками.

Таким образом, тенденция к усилению государственного контроля над трансграничной передачей данных является доминирующей, даже в тех юрисдикциях, которые формально придерживаются либеральных или условных принципов.

Список литературы:

[1] Восс, У.Г. Трансграничные потоки данных, общий регламент защиты персональных данных и управление данными / У.Г. Восс // Вестник международных организаций. 2022. Т. 17. № 1. С. 56–95 (на русском языке). doi:10.17323/1996-7845-2022-01-03

[2] Регламент Европейского Парламента и Совета Европейского Союза 2016/679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС (Общий Регламент о защите персональных данных / General Data Protection Regulation /GDPR)

[3] Лю Ц. Роль трансграничных потоков данных в развитии цифровой экономики и мировой торговли / Ц. Лю // Инновации и инвестиции. 2025. № 3. С. 81–84. EDN: NUQMAN

[4] Асадуллина, А.В. Проблемы регулирования трансграничных потоков данных в мировой экономике / А.В. Асадуллина // Российский внешнеэкономический вестник. 2021. № 1. С. 51–59. EDN: DWJWPM

[5] Исмагилова, О.Д., Хаджи, К.Р. Мировой опыт регулирования защиты, передачи и хранения данных / О.Д. Исмагилова, К.Р. Хаджи // Экономическая политика. 2020 Т. 15 № 3 С. 152–175 DOI: 10.18288/1994-5124-2020-3-152-175

[6] Чжао, Л. Основные модели режимов трансграничной передачи данных: ЕС, США и КНР / Л. Чжао // Право и политика. 2024. № 4. С. 50–60. DOI: 10.7256/2454-0706.2024.4.70797

[7] Ларионова, М.В. Возможно ли лидерство «группы двадцати» по вопросам управления данными? Есть ли шанс на сближение подходов? / М.В., Шелепов А.В. Ларионова // Вестник международных организаций: образование, наука, новая экономика. – 2023. – Т. 18. № 1. – С. 7–32. DOI: 10.17323/1996-7845-2023-01-01

[8] Смирнов, Е.Н. Вызовы глобального регулирования международной цифровой торговли / Е.Н. Смирнов // Торговая политика. 2020. №1/21. С. 25–33 doi:10.17323/2499-9415-2020-25-33

[9] Peters M. Digital trade, digital economy and the digital economy partnership agreement (DEPA) Educational Philosophy and Theory. 2022. Vol. 55(7), pp. 747–755, URL: <https://doi.org/10.1080/00131857.2022.2041413>

[10] Всеобъемлющее и прогрессивное соглашение о Транстихоокеанском парт-нерстве : текст соглашения // Центр для ВТО и международной торговли Министерства коммерции и промышленности Вьетнама. [Электронный ресурс]. URL: <https://wtocenter.vn/chuyen-de/12782-full-text-of-cptpp> (дата обращения: 30.06.2023).

[11] Aaronson S. A., Leblond P. Another Digital Divide: The Rise of Data Realms and its Implications for the WTO. Journal of International Economic Law. 2018. Vol. 21(2), pp. 245–272. URL: <https://doi.org/10.1093/jiel/jgy019>

[12] OECD/WTO (2025), Economic Implications of Data Regulation: Balancing Openness and Trust, OECD Publishing, Paris, <https://doi.org/10.1787/aa285504-en>.

[13] Оценка интеграционных процессов ЕАЭС в сфере торговли: 2024.Международный доклад НИУ ВШЭ / М. К. Глазатова (рук. авт. кол.), Д. Г. Абуова, С. С. Аветисян, Д. Н. Ахвердян и др. ; Нац. исслед. ун-т«Высшая школа экономики». — М. : Изд. дом Высшей школы экономики, 2024. — 350 с.

[14] Решение суда ЕС от 06.10.2015 по делу № C-362/14 (Максимиллиан Шремс против Уполномоченного по защите данных)

[15] Personal Information Protection Law of the People's Republic of China (Adopted at the 30th Meeting of the Standing Committee of the Thirteenth National People's Congress on August 20, 2021)

[16] Ferracane M. F., Lee-Makiyama H., van der Marel E. Digital Trade Restrictiveness Index. European Centre for International Political Economy (ECIPE). 2018. URL: https://ecipe.org/wp-content/uploads/2018/05/DTRI_FINAL.pdf

References:

[1] Voss, U.G. Cross-Border Data Flows, General Regulation on the Protection of Personal Data and Data Management/U.G. Voss//Bulletin of International Organizations. 2022. VOL. 17. № 1. S. 56–95 (in Russian). doi:10.17323/1996-7845-2022-01-03

[2] European Parliament and Council Regulation 2016/679 of 27 April 2016 on the protection of natural persons in the processing of personal data and on the free circulation of such data, and on the repeal of Directive 95/46/EC (General Data Protection Regulation/GDPR)

[3] Liu C. The role of cross-border data flows in the development of the dig-ital economy and world trade/C. Liu//Innovation and investment. 2025. № 3. S. 81-84. EDN: NUQMAH

[4] Asadullina, A.V. Problems of regulation of cross-border data flows in the global economy/A.V. Asadullina//Russian Foreign Economic Bulletin. 2021. № 1. S. 51-59. EDN: DWJWPM

[5] Ismagilova, O.D., Hadji, K.R. World experience in regulating protection, transmission and data storage/O.D. Ismagilova, K.R. Hadji//Economic poli-cy. 2020 VOL. 15 NO. 3 S. 152-175 DOI: 10.18288/1994-5124-2020-3-152-175

[6] Zhao, L. Main models of cross-border data transfer regimes: EU, USA and PRC/L. Zhao//Law and policy. 2024. № 4. S. 50-60. DOI: 10.7256/2454-0706.2024.4.70797

[7] Larionova, M.V. Is G20 Leadership on Data Management Possible? Is there a chance for rapprochement of approaches ?/M.V., Shelepov A.V. La-ri-onova//Bulletin of international organizations: education, science, new economy. – 2023. - VOL. 18. № 1. - S. 7-32. DOI: 10.17323/1996-7845-2023-01-01

[8] Smirnov, E.N. Challenges of global regulation of international digital trade/E.N. Smirnov//Trade policy. 2020. №1/21. P. 25-33 doi: 10.17323/ 2499-9415-2020-25-33

[9] Peters M. Digital trade, digital economy and the digital economy part-nership agreement (DEPA) Educational Philosophy and Theory. 2022. Vol. 55(7), pp. 747–755, URL: <https://doi.org/10.1080/00131857.2022.2041413>

[10] Comprehensive and progressive agreement on Trans-Pacific Partner-ship: text of the agreement//Center for WTO and International Trade of the Ministry of Commerce and Industry of Vietnam. [Electronic resource]. URL: <https://wtocenter.vn/chuyen-de/12782-full-text-of-cptpp> (access date: 30.06.2023).

[11] Aaronson S. A., Leblond P. Another Digital Divide: The Rise of Data Realms and its Implications for the WTO. Journal of International Eco-nomic Law. 2018. Vol. 21(2), pp. 245–272. URL: <https://doi.org/10.1093/jiel/jgy019>

[12] OECD/WTO (2025), Economic Implications of Data Regulation: Bal-ancing Openness and Trust, OECD Publishing, Paris, <https://doi.org/10.1787/aa285504-en>.

[13] Assessment of the EAEU integration processes in the field of trade: 2024. International report of the Higher School of Economics/M. K. Glaza-tov (hand. aut. col.), D. G. Abuova, S. S. Avetisyan, D. N. Akhverdyan and others; Nat. †. University “Higher School of Economics.” - M.: Ed. House of the Higher School of Economics, 2024. - 350 s.

[14] EU Court of 06.10.2015 Decision in Case No. C-362/14 (Maximillian Schrems v. Data Protection Commissioner)

[15] Personal Information Protection Law of the People's Republic of China (Adopted at the 30th Meeting of the Standing Committee of the Thirteenth National People's Congress on August 20, 2021)

[16] Ferracane M. F., Lee-Makiyama H., van der Marel E. Digital Trade Restrictiveness Index. European Centre for International Political Economy (ECIPE). 2018. URL: https://ecipe.org/wp-content/uploads/2018/05/DTRI_FINAL.pdf



ЮРКОПАНИ

www.law-books.ru

Юридическое издательство «ЮРКОПАНИ»
издает научные журналы:

- Научно-правовой журнал «Образование и право», рекомендованный ВАК Министерства науки и высшего образования России (специальности 12.00.01, 12.00.02), выходит 1 раз в месяц.
- Научно-правовой журнал «Право и жизнь», рецензируемый (РИНЦ, E-Library), выходит 1 раз в 3 месяца.