

Кочетов Иван Максимович,

юрисконсульт ГБУ «Озеленение», Россия, г. Москва

Семеновских Александр Михайлович,

юрисконсульт АО «ДИКСИ Юг», Россия, г. Москва

Научный руководитель: Гулиева Мехрибан Эльбрус кызы,

кандидат юридических наук, доцент кафедры международного и публичного права юридического факультета Финансового университета при Правительстве Российской Федерации

**ЦИФРОВОЙ СУВЕРЕНИТЕТ И ГЕОПОЛИТИКА ДАННЫХ:
ФОРМИРОВАНИЕ НОВОГО ЛАНДШАФТА МЕЖДУНАРОДНОГО
ЭКОНОМИЧЕСКОГО ПРАВА**

Аннотация: Цифровая трансформация мировой экономики привела к возникновению феномена цифрового суверенитета как способности государства контролировать данные на своей территории и определять правила их трансграничного перемещения. В статье исследуется влияние геополитики данных на эволюцию международного экономического права, анализируются конфликты юрисдикций, региональные модели регулирования и противоречия между принципами свободной торговли и требованиями национальной безопасности. Обосновывается вывод о том, что традиционные механизмы международного экономического права, включая инструменты ВТО, уже недостаточны для регулирования цифровых потоков данных, что ведет к фрагментации правового пространства и формированию новых норм международного взаимодействия.

Ключевые слова: цифровой суверенитет, геополитика данных, международное экономическое право, трансграничная передача данных, цифровая юрисдикция, локализация данных, кибербезопасность.

Annotation: *The digital transformation of the global economy has led to the emergence of digital sovereignty as a state's ability to control data within its territory and determine the rules governing cross-border data flows. The article examines the influence of data geopolitics on the evolution of international economic law, analyses jurisdictional conflicts, regional regulatory models, and contradictions between free trade principles and national security requirements. It is argued that traditional mechanisms of international economic law, including WTO instruments, are no longer sufficient to regulate digital data flows, which results in legal fragmentation and the formation of new norms of international interaction.*

Key words: *digital sovereignty, data geopolitics, international economic law, cross-border data flows, digital jurisdiction, data localization, cybersecurity.*

Данные как объект геополитического противостояния

Начало XXI века ознаменовалось радикальной трансформацией представлений о стратегических ресурсах. Если прежде мировая политика вращалась вокруг контроля над территориями, энергоносителями и транспортными путями, то цифровизация экономики выдвинула на первый план новый объект — данные. Объёмы генерируемой информации удваиваются каждые два года: только в 2024 году мировой цифровой трафик превысил 149 зеттабайт [1]. При этом географическое распределение центров обработки данных остаётся крайне неравномерным — около 60% дата-центров размещены в США, странах ЕС и Китае.

Российская Федерация относительно поздно, по сравнению с рядом западных стран, осознала критическую важность информационного суверенитета, однако предпринятые шаги демонстрируют поступательное движение к формированию национальной модели регулирования. Принятие в 2015 году Федерального закона № 242-ФЗ о локализации персональных данных стало запоздалой, но необходимой реакцией на доминирование

иностранных технологических платформ [2]. Практика подтверждает: зависимость от зарубежных облачных сервисов и социальных сетей создаёт уязвимости не только для национальной безопасности, но и для экономической автономии государства. По данным МВД России, только за январь-июль 2023 года число цифровых преступлений выросло почти на 30%, большинство из них совершается с использованием сети Интернет [3].

Данные перестали быть сугубо технической категорией – это инструмент влияния, прогнозирования социальных процессов и управления ими. Крупнейшие технологические корпорации фактически присвоили себе функции, традиционно принадлежавшие государствам: мониторинг коммуникаций, формирование информационной повестки, определение стандартов цифрового взаимодействия.

Показательна история с экстерриториальным применением американского законодательства. CLOUD Act 2018 года предоставил правоохранительным органам США право требовать доступ к данным, хранящимся на серверах американских компаний, независимо от их физического местонахождения [4]. Это вступает в противоречие с принципом территориального суверенитета, закрепленным в ст. 2 Устава ООН, и порождает коллизии юрисдикций.

Европейский Союз избрал путь жесткого комплаенса. Общий регламент по защите данных (GDPR), вступивший в силу в мае 2018 года, установил беспрецедентно строгие требования к обработке персональных данных. Штрафы достигают 4% глобальной выручки компании — суммы, заставляющие даже технологических гигантов пересматривать свои бизнес-модели [5]. Как следует из сводных отчетов EDPB на начало 2025 года, совокупный объём санкций, наложенных европейскими регуляторами, превысил 4,8 млрд евро [6]. Параллельно действует Конвенция Совета Европы №108, определяющая персональные данные, как любую информацию об определенном или поддающемся определению физическом лице. Именно это

определение легло в основу ст.3 Федерального закона №152-ФЗ, однако, как справедливо отмечает В.И. Солдатова, широкое толкование создает проблемы квалификации, что ведет к судебным спорам [7].

Китайская Народная Республика демонстрирует наиболее жёсткую модель цифрового суверенитета. Закон о кибербезопасности 2017 года и Закон о защите персональных данных 2021 года создали систему, где государство в лице уполномоченных органов имеет легитимный доступ к данным, циркулирующим на национальной территории, при наличии судебного или административного решения. Особого внимания заслуживает инфраструктура «социального кредита», аккумулирующая персональные данные физических и юридических лиц через различные виды мониторинга, что, по оценке Д.Б. Велиуловой, ведет к перманентному росту доступа правительства Китая к персональным данным [8].

Россия движется в направлении формирования собственной модели, которая стремится совместить экономическую эффективность с требованиями безопасности. Концепция цифрового суверенитета, закреплённая в Федеральном законе № 90-ФЗ от 01.05.2019 и Стратегии развития информационного общества на 2017-2030 годы, предполагает создание автономной, но не изолированной цифровой среды [9]. Речь идёт не о построении «цифровой крепости», а о способности государства гарантировать устойчивость критической информационной инфраструктуры даже в условиях внешнего давления. Вместе с тем дополнительные риски создает низкий уровень цифровых компетенций населения. По данным НАФИ от 2022г. базовым уровнем цифровой грамотности обладают 69% процентов россиян, продвинутым – лишь 29%, самые низкие показатели в умении обеспечивать защиту своих персональных данных [10].

Кризис классического международного экономического права

Традиционные механизмы регулирования международной торговли формировались в эпоху, когда объектами экономического обмена были

материальные товары и чётко определённые услуги. Соглашения ВТО (ГАТТ, ГАТС) базируются на принципах недискриминации, национального режима и режима наибольшего благоприятствования. Однако цифровая экономика бросает вызов этим фундаментальным принципам.

Возьмём категорию «товар». Являются ли данные товаром в классическом понимании? Программное обеспечение распространяется через скачивание — это услуга или товар? Облачные вычисления предоставляют удалённый доступ к инфраструктуре — какая классификация здесь применима? Существующие определения размываются, создавая зоны правовой неопределённости.

Принцип свободы торговли, постулат либерального экономического порядка, вступает в противоречие с требованиями локализации данных. Когда государство обязывает компанию хранить данные своих граждан на национальной территории, это рассматривается как барьер для торговли. Но одновременно это легитимная мера защиты суверенитета. Где проходит граница между протекционизмом и обоснованной озабоченностью безопасностью?

Российская практика последних лет наглядно демонстрирует эту дилемму. Требование о размещении серверов на территории РФ привело к уходу ряда зарубежных компаний, но одновременно стимулировало развитие отечественной индустрии дата-центров. Объём инвестиций в эту сферу вырос с 27 млрд рублей в 2020 году до 89 млрд рублей в 2024 году [11]. Это ограничение торговли или стратегическое инвестирование в технологическую независимость?

Попытки адаптировать правовую базу ВТО к цифровой реальности натываются на непреодолимые разногласия. Инициатива Joint Statement Initiative on Electronic Commerce, запущенная в 2019 году, объединила 86 государств-членов ВТО, но за пять лет переговоров не привела к консенсусу. Позиции слишком различны. США настаивают на полной либерализации

трансграничных потоков данных. Европейский Союз требует включения норм о защите прав. Развивающиеся страны опасаются, что свобода данных закрепит доминирование технологических гигантов Севера.

Китай и Россия выступают за признание права государств регулировать цифровое пространство в соответствии с национальными интересами. Это не отрицание международного сотрудничества, а требование признать многообразие моделей развития. Тезис о «суверенном интернете» воспринимается западными аналитиками как угроза открытому цифровому пространству, но с точки зрения незападных стран — это защита от информационной гегемонии.

Налицо фрагментация правового ландшафта. Вместо единой системы правил формируются региональные и двусторонние режимы. Соглашение между США и Японией о цифровой торговле 2019 года, цифровые главы в торговых соглашениях ЕС, Всестороннее региональное экономическое партнёрство (RCEP) — каждое из этих соглашений устанавливает собственные нормы. Результат — мозаичность, непредсказуемость, рост транзакционных издержек для бизнеса.

Парадокс ситуации в том, что принцип правовой определённости — основа любого международного регулирования — подрывается самой динамикой технологического развития. Законы пишутся годами, технологии меняются месяцами. Блокчейн, искусственный интеллект, квантовые вычисления — каждая новая волна инноваций ставит вопросы, на которые международное право не имеет готовых ответов.

Новые нормы и институты: контуры формирующегося порядка

Кризис не означает хаоса. Скорее, мы наблюдаем болезненный процесс формирования нового нормативного порядка, адекватного реалиям цифровой эпохи. Этот процесс идёт не сверху вниз (от международных организаций к государствам), а снизу вверх — через практику, двусторонние соглашения, региональные инициативы.

Концепция «доверенных данных» (trusted data flows) постепенно занимает центральное место в дискуссиях. Суть её в том, что трансграничные потоки данных допустимы между государствами, которые обеспечивают сопоставимый уровень защиты. Европейский Союз развивает эту логику через механизм решений об адекватности (adequacy decisions), позволяющих передавать данные в третьи страны, чьё законодательство соответствует стандартам GDPR. К началу 2025 года такие решения приняты в отношении 14 юрисдикций, включая Японию, Южную Корею, Великобританию.

Россия пытается встроиться в эту систему через соглашения о сотрудничестве в области обмена данными с партнёрами по ЕАЭС и БРИКС. Формирование единого цифрового пространства Евразийского экономического союза предполагает гармонизацию законодательства о защите данных [12]. Впрочем, реальный прогресс здесь медленный — слишком различны уровни цифрового развития государств-членов.

Институционально возникают новые структуры. Рабочая группа ООН по цифровой экономике, созданная в рамках ЮНКТАД, пытается выработать базовые принципы регулирования. Инициатива «Цифровой шёлковый путь», продвигаемая Китаем, предлагает альтернативную модель технологического сотрудничества, ориентированную на развивающиеся страны. Партнёрство по цифровой экономике (Digital Economy Partnership Agreement), объединяющее Чили, Новую Зеландию и Сингапур, разрабатывает гибкие механизмы регулирования трансграничных данных.

Российские исследователи справедливо отмечают, что эти разрозненные инициативы не складываются в целостную систему [2]. Отсутствует общепризнанная иерархия норм, механизмы разрешения споров между различными режимами, институты, способные обеспечить исполнение решений. Речь идёт скорее о сетевом управлении (network governance), где взаимодействуют государственные и негосударственные акторы, формальные и неформальные правила, национальные и транснациональные структуры.

Показательна роль технологических корпораций. Google, Meta (признана экстремистской и запрещена в РФ), Amazon не просто объекты регулирования — они сами становятся регуляторами, устанавливая стандарты безопасности, правила модерации контента, условия доступа к платформам. Возникает феномен «частного управления» (private governance), когда нормы создаются не государствами, а корпорациями. Это вызов Вестфальской модели, где суверенитет неразрывно связан с государством.

Вопрос о балансе между инновациями и регулированием остаётся центральным. Избыточное регулирование душит технологическое развитие. Отсутствие регулирования создаёт риски монополизации и злоупотреблений. Европейская модель делает ставку на строгие правила (GDPR, Digital Markets Act, Digital Services Act). Американская — на саморегулирование и рыночную конкуренцию. Китайская — на государственный контроль при поддержке национальных чемпионов. Российская модель пока находится в поиске собственной идентичности, балансируя между европейским акцентом на защиту данных и китайским вниманием к безопасности.

Судебная практика также формирует новые нормы. Решение Суда Европейского Союза по делу Schrems II (июль 2020 года), признавшее недействительным механизм «Щита конфиденциальности» (Privacy Shield) для передачи данных в США, продемонстрировало готовность судов защищать цифровой суверенитет даже в ущерб трансатлантическим экономическим связям [4]. Российские суды также начинают вырабатывать подходы к определению юрисдикции в цифровых спорах, хотя практика пока не столь обширна.

Криптографические технологии и блокчейн могут изменить саму логику проблемы. Если данные технически защищены и децентрализованы, вопрос о локализации теряет смысл. Но одновременно возникают новые риски: невозможность государственного контроля, использование технологий для незаконной деятельности, сложность налогообложения криптоактивов.

Регулирование блокчейна и криптовалют — следующая большая проблема для международного экономического права, и консенсуса здесь нет даже в зачаточной форме.

Заключение

Цифровизация экономики демонтирует привычную архитектуру международного экономического права. Данные как объект регулирования не вписываются в категории, разработанные для материальных товаров и традиционных услуг. Принципы свободной торговли сталкиваются с императивами национальной безопасности и цифрового суверенитета. Механизмы ВТО оказываются неадекватными новым вызовам.

Формирующийся правовой ландшафт характеризуется фрагментацией и конкуренцией моделей. Европейский акцент на защите персональных данных, американская приверженность свободе потоков информации, китайская модель государственного контроля, российский поиск баланса между открытостью и безопасностью — эти подходы пока не синтезируются в единую систему. Результат — мозаичность правового пространства, рост неопределённости для бизнеса, риски эскалации цифровых конфликтов.

Россия находится на критическом этапе формирования собственной стратегии. С одной стороны, требования технологической независимости и защиты критической инфраструктуры диктуют жёсткое регулирование. С другой стороны, изоляция от глобальных цифровых потоков чревата технологическим отставанием и экономическими потерями. Поиск оптимального баланса — задача ближайших лет.

Перспективы формирования универсальных правил цифровой торговли остаются туманными. Вероятнее развитие сетевой системы двусторонних и региональных соглашений, основанных на принципе «доверенных потоков» между государствами со сходными стандартами. Это не идеал универсального порядка, но реалистичный сценарий для переходного периода.

Дальнейшие исследования должны сосредоточиться на разработке конкретных механизмов совместимости различных правовых режимов, анализе судебной практики по цифровым спорам, оценке эффективности существующих инструментов регулирования. Геополитика данных — это не временный феномен, а долгосрочная трансформация международных экономических отношений, требующая переосмысления базовых категорий права и политики.

Список литературы:

1. Прогноз развития цифровой экономики до 2030 года: аналитический доклад // Институт исследований развития цифровой экономики РАНХиГС. М.: Дело, 2025. 156 с.
2. Иванов А.С., Петрова М.В. Цифровой суверенитет как элемент национальной безопасности Российской Федерации // Национальные интересы: приоритеты и безопасность. 2024. Т. 20. № 4. С. 678-693. URL: <https://elibrary.ru/item.asp?id=56892341> (дата обращения: 15.04.2026).
3. Характеристика состояния преступности в Российской Федерации за январь-декабрь 2023 года: официальный сайт МВД РФ. – URL: <https://xn--b1aew.xn--p1ai/reports/item/40874008/> (дата обращения: 04.04.2026).
4. Полякова Т.А. Правовое регулирование трансграничной передачи персональных данных в условиях цифровизации // Журнал российского права. 2023. № 7. С. 134-147.
5. Васильева Е.Н. Европейский регламент GDPR и его влияние на российское законодательство о персональных данных // Вестник Санкт-Петербургского университета. Право. 2023. Т. 14. № 2. С. 456-472. URL: <https://elibrary.ru/item.asp?id=53284567> (дата обращения: 15.04.2026).
6. Годовой отчет EDPB за 2024 год: официальный сайт European data protection board. – URL: <https://www.edpb.europa.eu/our-work-tools/our->

documents/annual-report/edpb-annual-report-2024_en (дата обращения: 04.04.2026).

7. Солдатова В. И. Защита цифровых данных в условиях применения цифровых технологий // Lex Russica. - 2020. – Т. 73, №2 (159). – С. 33-43.

8. Велиулова Д.Б. Правовой режим защиты и охраны персональных данных в национальных законодательствах // Журнал зарубежного законодательства и сравнительного правоведения. – 2023. – Т.19, №6. – С. 123-129.

9. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы: утв. Указом Президента РФ от 09.05.2017 № 203 // Собрание законодательства РФ. 2017. № 20. Ст. 2901.

10. В России выросла доля людей с продвинутым уровнем цифровой грамотности: официальный сайт НАФИ. URL: <https://nafii.ru/ratings/index-tsifrovoy-gramotnosti/?ysclid=mnkm3mgdgu365435502> (дата обращения: 04.04.2026).

11. Концепция развития отечественной индустрии дата-центров на период до 2030 года // Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. М., 2024. 87 с.

12. Якушев М.В. Формирование единого цифрового пространства ЕАЭС: правовые аспекты // Евразийская интеграция: экономика, право, политика. 2024. № 3. С. 89-104.