Право и политика
Правильная ссылка на статью:
Чжао Л. Основные модели режимов трансграничной передачи данных: ЕС, США и КНР // Право и политика. 2024. № 4. DOI: 10.7256/2454-0706.2024.4.70797 EDN: WNDYGF URL: https://nbpublish.com/library_read_article.php?id=70797

Основные модели режимов трансграничной передачи данных: ЕС, США и КНР

Чжао Лэй

ORCID: 0000-0002-9108-1007

аспирант; кафедра сравнительной политологии; Российский университет дружбы народов

117279, Россия, г. Москва, ул. Миклухо-Маклая, 6

1651847660@qq.com

Статья из рубрики "Трансформация правовых и политических систем"

DOI:

10.7256/2454-0706.2024.4.70797

EDN:

WNDYGF

Дата направления статьи в редакцию:

19-05-2024

Дата публикации:

27-05-2024

Аннотация: Предметом исследования данной статьи является система регулирования трансграничных потоков данных и ее правовой режим. Данные являются фундаментальным ресурсом для развития цифровой экономики. Сегодня, когда большое развитие получила глобализация, в международной торговле неизбежно наличие трансграничных потоков данных. Однако передача данных за границу создает скрытые угрозы для конфиденциальности личной информации граждан и национальной безопасности. Многие страны создали системы управления передачей данных, чтобы защитить собственные интересы. Зрелые режимы управления передачей данных за границу часто становятся примером для других стран. Принятые законы также послужили образцом для других стран. Наиболее репрезентативные режимы на сегодняшний день существуют в ЕС, США и Китае, которые демонстрируют три пути

управления данными. Цель данной статьи – сравнить режимы трансграничной передачи данных в Европейском союзе, США и Китае, чтобы проанализировать структуру трех репрезентативных режимов, а также изучить причины их формирования и последствия функционирования. Рассмотрение трех систем позволяет более четко показать, что Европейский союз, США и Китай имеют различные ценностные ориентации, которые непосредственно привели к формированию трех различных правовых систем. Свободный рынок и национальная безопасность стали основными элементами национальных соображений при разработке законов о трансграничных данных. На основе проведенного исследования можно сделать вывод, что режим трансграничной передачи данных в ЕС является наиболее полным и эффективным, обладая демонстрационным эффектом. Китайская система в настоящее время имеет серьезные недостатки. А закон США в последние годы все больше ориентирован на служение интересам геополитики. Законы о трансграничной передаче данных демонстрируют тенденции политической инструментализации. Балканизация Интернета становится все более очевидной.

Ключевые слова:

трансграничная передача данных, киберсуверенитет, суверенитет данных, ЕС, США, КНР, Балканизация Интернета, Управление данными, безопасность данных, цифровая экономика

Введение

В XXI веке цифровые технологии произвели революцию в производстве и жизни людей. В январе 2024 года число пользователей Интернета в мире достигло 5,35 миллиарда человек, что составляет 66,2 процента от всего населения планеты [1]. Мир вступил в цифровую эпоху. По данным Всемирного банка, в 2022 году доля цифровой экономики в мировом ВВП превысила 15 процентов, в последнее десятилетие она росла в 2,5 раза быстрее, чем ВВП физического мира [2]. Высокие технологии, такие как большие данные, искусственный интеллект, интернет вещей и блокчейн, занимают лидирующие позиции в мире. Являясь продуктом цифровых технологий, данные стали пятым по значимости фактором производства наравне с землей, трудом, капиталом и технологиями. Данные теперь составляют основу для дальнейшего развития цифровых технологий, а контроль над данными и их защита являются важнейшим приоритетом правительств. С увеличением частоты транснациональной экономической и социальной деятельности постепенно увеличивается объем трансграничной передачи данных, что, несомненно, порождает ряд проблем безопасности, таких как кража данных, нарушение неприкосновенности частной жизни и утечка коммерческой тайны. Поэтому создание ряда систем правового регулирования передачи данных за границу – это вопрос, который необходимо решить каждой стране. В связи с ресуверенизацией киберпространства концепция суверенитета данных была принята многими странами и стала одной из основных концепций управления данными. В настоящее время отсутствует единая глобальная модель управления трансграничными потоками данных, и каждая страна имеет собственную степень цифрового развития и по-своему ориентирована на защиту собственных интересов, что приводит к большим различиям в действующем законодательстве по передаче данных за границу. США и Европейский союз ранее проводили законодательную работу в области трансграничной передачи данных, их правовые системы более совершенны и являются двумя основными парадигмами права в области данных. Цифровые технологии и цифровая экономика

Китая в последние годы стремительно развиваются, но китайское законодательство в области данных появилось не так давно. В настоящее время в Китае создан комплекс правовых систем в области передачи данных за границу, призванный решить проблемы, возникающие в данной сфере, в том числе проблему безопасности данных. Три режима данных представляют собой три системы ценностных ориентаций, а также являются наиболее показательными примерами глобального управления процессами трансграничной передачи данных.

Режимы управления и ключевые законы в области трансграничной передачи данных в ЕС, США и КНР

В отличие от традиционных ресурсов, данные неосязаемы, мобильны и не подлежат потреблению. Данные могут использоваться различными лицами и предприятиями на разных стадиях производства и потребления, и они приносят больше выгод, чем обычные ресурсы [3]. Но данные, с одной стороны, создаются субъектами, такими как люди или организации, а с другой – требуют хранения. И они находятся в пределах национальных границ. Общепринято, что суверенитет данных является подмножеством киберсуверенитета [4]. Согласно определению суверенитета, субъекты данных, носители данных, действия с данными и ресурсы данных внутри страны находятся под юрисдикцией национального правительства в пределах национальных границ страны; за ее пределами национальное правительство обладает автономией и имеет независимый и равный статус наряду с другими национальными правительствами.

В области управления данными законодательство ЕС часто заимствует опыт других стран, его законодательную историю можно проследить с Конвенции о защите физических лиц при автоматизированной обработке персональных данных (Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 1981) и Директивы о защите физических лиц при обработке персональных данных и о свободном обращении таких данных (Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the free Movement of such Data, Directive 95/46/EC, 1995). В последнем документе ЕС впервые ввел стандартное требование «адекватного уровня защиты» для стран, не являющихся членами ЕС, как получателей данных, – правило, которое действует и в настоящее время.

В ответ на развитие цифровых технологий 14 апреля 2016 года Совет Европейского союза принял Общий регламент по защите данных (General Data Protection Rules, GDPR) [5], который вступил в силу 25 мая 2018 года и заменил собой Директиву 95/46/EC. GDPR – обязательный закон, который требует прямого и единообразного действия во всех странах-членах ЕС и не требует от правительств стран-участниц ЕС никаких изменений в локальных законодательствах, что позволяет создать гармоничный режим защиты данных. По сравнению с Directive 95/46/EC, GDPR расширяет сферу действия суверенитета над данными, включая компании, расположенные за пределами ЕС, но имеющие операционное присутствие в ЕС и обслуживающие субъекты на территории ЕС. Штрафы за нарушение GDPR, по сравнению с предыдущими законами, были значительно увеличены, что также повышает эффективность GDPR.

Теоретически GDPR представляет собой территориальный закон, основополагающими границами которого является весь Европейский союз. В законе проводится строгое различие между государствами-членами ЕС и государствами, не являющимися членами ЕС. Статья 46 главы V гласит, что передача персональных данных странам или международным организациям за пределами ЕС разрешена только в том случае, если

уровень защиты данных в стране-получателе был оценен как сопоставимый с уровнем защиты данных в ЕС или если страна-получатель входит в список стран, «защищенных надлежащим образом» согласно GDPR. В GDPR прямо указано, что обработка персональных данных обработчиками или контролерами, чьи организации созданы в ЕС, подпадает под действие GDPR, независимо от того, происходит ли действие в ЕС, что отражает как принцип территориальности, так и принцип индивидуальности. Поэтому можно утверждать, что фактически GDPR действует и за пределами ЕС. В целом, в управлении данными в ЕС преобладает территориальная юрисдикция, дополняемая персональной юрисдикцией [6]. Его основная цель – защита персональных данных в ЕС. Можно сказать, что закон носит консервативный характер. В последние годы новые законы, такие как недавно принятый законопроект об управлении данными и Закон о данных, способствовали дальнейшему совершенствованию системы управления данными в ЕС.

По сравнению с ЕС, законодательство США в области передачи данных за границу более фрагментировано. С одной стороны, в США обычно принимаются отдельные законы по отраслям, например, Закон о праве на финансовую неприкосновенность частной жизни (Right to Financial Privacy Act of 1978) и Закон о финансовой модернизации (Financial Services Modernization Act of 1999) в финансовом секторе, Правила администрирования экспорта (Export Administration Regulations) и Закон о реформе экспортного контроля (Export Control Reform Act of 2018), Закон о модернизации оценки рисков иностранных инвестиций (Foreign Investment Risk Review Modernization Act of 2018) в инвестиционном секторе; с другой стороны, отдельные штаты США обладают независимыми законодательными полномочиями, например, штаты Калифорния, Вашингтон, Колорадо, Вирджиния имеют местные законодательные положения о конфиденциальности личной информации. Наиболее важным законом в области управления данными в США является Clarifying Lawful Overseas Use of Data Act (CLOUD Act)[7], который был принят в 2018 году с целью урегулирования судебного процесса правительства США против Microsoft. Закон наделяет правительство США правом доступа и получения данных, хранящихся у интернет-провайдеров на территории страны и в любом месте за ее пределами.

Закон CLOUD предусматривает, что данные, контролируемые контролером данных, подпадают под юрисдикцию США, если контролер данных является лицом США (гражданином США или американской компанией). Это отражает тот факт, что Закон CLOUD основан на принципе гражданства. Согласно Закону, Соединенные Штаты могут напрямую получить доступ к данным, хранящимся у американских компаний в других странах, а тот факт, что американские интернет-компании работают по всему миру, делает юрисдикцию «длинной руки», предусмотренную Законом о CLOUD, распространяющейся на большинство стран по всему миру.

В июне 2015 года Постоянный комитет Всекитайского собрания народных представителей 12-го созыва принял Закон о кибербезопасности Китайской Народной Республики, в котором говорится, что операторы критической инфраструктуры обязаны проводить оценку безопасности при предоставлении важных данных за пределами страны, за исключением случаев, когда это предусмотрено другими законами. Закон о кибербезопасности, а также Закон о безопасности данных и Закон о защите личной информации, которые впоследствии были приняты в качестве законодательных актов, представляют собой основные законы о трансграничной передаче данных в Китае. Эти законы завершают разработку верхнего уровня китайского режима передачи данных за границу.

Что касается конкретной реализации политических мер, то специальные положения содержатся в подзаконных актах, таких как Меры по оценке безопасности экспорта данных, Правила осуществления сертификации защиты персональных данных и Меры по заключению стандартных договоров на экспорт персональных данных. Например, такие данные, как важные данные, крупномасштабные персональные данные и персональные данные, обрабатываемые операторами критических информационных инфраструктур, отвечают требованиям Мер по оценке безопасности экспорта данных, а такие данные, как неважные данные, персональные данные малого и среднего размера и персональные данные, обрабатываемые операторами некритических информационных инфраструктур, должны отвечать требованиям Правил осуществления сертификации защиты персональных данных и Мер по заключению стандартных договоров на экспорт персональных данных. Китай также разработал целевое законодательство в специализированных областях знаний, например, Меры по управлению борьбой с отмыванием денег и финансированием терроризма для финансовых учреждений, Положения об управлении генетическими ресурсами человека и Меры по управлению данными о здоровье населения. Можно утверждать, что множество законодательных актов разного уровня в совокупности представляют собой сложную китайскую систему управления трансграничной передачей данных.

Ценностные ориентации и причины принятия законов в области трансграничной передачи данных в ЕС, США и Китае

Разработка национальной политики и законов должна основываться на объективной ситуации в стране, а также отвечать национальным интересам. Объективные национальные условия в ЕС, США и Китае сильно отличаются, как и их национальные интересы, поэтому и правовые системы, которые в итоге формируются, имеют значительные различия.

ЕС придает большое значение правам отдельных граждан в процессе управления данными и рассматривает их личные данные как проекцию власти граждан в онлайн-мире. Защита основных прав граждан ЕС является обязанностью ЕС. Обработка данных, содержащих большое количество личной информации, несомненно, создает риск нарушения прав граждан. Поэтому в GDPR ЕС отражена идея консерватизма и закреплено право граждан на забвение [8]. Основываясь на защите личной жизни, ЕС устанавливает жесткие ограничения на передачу данных за границу и фактически возводит высокую стену для передачи данных. Защита индивидуальных прав и неприкосновенности частной жизни также защищает безопасность ЕС в цифровой сфере, предотвращая утечку критически важной информации из ЕС за его пределы.

В начале цифровой эпохи компании из ЕС были конкурентоспособны на цифровом рынке и даже занимали лидирующие позиции в отрасли, но с углублением цифровых технологий европейские цифровые компании, представленные в том числе Nokia, проиграли и были вытеснены из конкурентной борьбы с американскими и китайскими компаниями. Однако ЕС, как один из самых развитых регионов мира, обладает огромным цифровым потребительским рынком с населением более 400 миллионов человек. На этот рынок ЕС опирается в своей борьбе за право устанавливать правила в глобальном цифровом управлении.

На основании GDPR и последующего «Закона о цифровых рынках» – Digital Markets Act (DMA), ЕС установил ряд критериев доступа на рынок. Для выхода на рынок ЕС цифровые компании из других стран должны соблюдать правила обработки данных ЕС. Оффшорные компании обязаны соблюдать GDPR при обработке данных пользователей из

ЕС, независимо от того, происходит ли это действие внутри или за пределами ЕС. GDPR имеет хорошо развитый механизм наказаний, поэтому компаниям сложно обойти этот мощный закон.

Эффективное и стабильное функционирование режима трансграничной передачи данных ЕС привело к тому, что многие страны признали защиту частной жизни и национальной безопасности, обеспечиваемую GDPR, который послужил образцом для разработки национальных режимов трансграничной передачи данных во многих странах. В процессе разработки законов другие страны часто ссылаются на установленные ЕС стандарты и взаимодействуют с ЕС на институциональном уровне. В результате транснациональные корпорации также стремятся соблюдать законодательные требования ЕС за его пределами, чтобы гармонизировать стандарты и снизить затраты на ведение бизнеса. ЕС использует рыночные механизмы для достижения «эффекта Брюсселя». Это привело к распространению стандартов ЕС с одностороннего на глобальный уровень, увеличивая власть ЕС на уровне регулирования.

Использование правил доступа на рынок для создания «эффекта Брюсселя» – распространенный способ расширения международного влияния ЕС. Например, чтобы ограничить монопольное поведение технологических гигантов на рынке ЕС, 5 июля 2022 года Европейский парламент принял DMA, который, как считается, направлен против основных цифровых платформ (gatekeepers) в ЕС в восьми областях: онлайн-поисковые системы, посреднические онлайн-услуги, социальные сети, платформы для обмена видео, коммуникационные платформы, рекламные услуги, операционные системы и облачные сервисы [9]. В число крупнейших компаний, участвующих в проекте, входят Alphabet, Amazon, Apple, ByteDance, Meta и Microsoft. Закон был положительно воспринят другими странами и регионами, включая Бразилию, Индию, Японию, Южную Корею и Великобританию, которые уже приняли или намереваются принять законодательство по модели DMA.

Поддержание экономической гегемонии всегда было ключевой стратегической задачей Соединенных Штатов, где давно существует идея свободной торговли. Сегодня, в цифровую эпоху данные стали одним из главных товаров. Свободный и быстрый трансграничный поток данных является основной предпосылкой для трансграничной цифровой торговли. Поэтому Соединенные Штаты поощряют свободный поток данных в глобальном масштабе. Исходя из этого, Соединенные Штаты просят другие страны снизить стандарты передачи данных за границу и не препятствовать передаче данных.

В отличие от ЕС, в США наиболее развита цифровая экономика, а американские технологические гиганты, представленные MAMAA (Meta, Apple, Microsoft, Alphabet, Amazon), доминируют во многих областях глобального цифрового рынка. Выступая за свободный поток данных, США могут собирать и использовать нужные им данные по всему миру благодаря монопольному положению технологических гигантов. Данные могут быть воспроизведены для ускорения технологического прогресса и увеличения экономических выгод, что способствует дальнейшему укреплению и усилению экономической гегемонии США.

Помимо экономических последствий, Соединенные Штаты могут достичь своих политических целей благодаря свободной торговле данными. Благодаря Закону CLOUD США пользуются принципом «длинной руки» для доступа к информации из других стран. Закон CLOUD не только дает правительству США юрисдикцию над гражданами, организациями или предприятиями США, но и позволяет правительству США получать доступ к данным из стран, субъекты которых принадлежат США. Это представляет

серьезную угрозу для суверенитета других стран в отношении данных. Поскольку американские интернет-компании работают по всему миру, США де-факто следят за глобальными данными, а широкая сфера действия закона CLOUD фактически является гегемонистской.

В последние годы в связи с изменением геополитической ситуации либеральная идеология США в области данных постепенно сменилась консерватизмом. Исходя из идеи геополитического противостояния, США устанавливают целевые барьеры для передачи данных за границу. Первоначально эта идея была воплощена в National Security and Personal Data Protection Act of 2019 (NSPDPA, пока не вступил в силу). Хотя этот закон не был реализован, его концепция запрета на передачу данных в страны, признанные угрозой безопасности США (Россия, Китай, Иран и др.), перекочевала в уже одобренный и принятый Protecting Americans' Data From Foreign Surveillance Act of 2023 и Protecting Americans' Data from Foreign Adversaries Act of 2024.

Для достижения собственных экономических и политических стратегических целей Соединенные Штаты стремятся продвигать стандарты свободной цифровой мобильности. Заключение двусторонних и многосторонних соглашений – основная мера, используемая Соединенными Штатами для продвижения своих идей на международном уровне. В зависимости от количества участников и региона, в котором они расположены, их можно разделить на двусторонние соглашения (Соглашение о свободной торговле между США и Чили), региональные многосторонние соглашения (Соглашение между США и Мексикой и Канадой) и соглашения международных организаций (Добровольная система трансграничных правил конфиденциальности). С помощью этих соглашений США продвигают собственные ключевые определения и основные принципы передачи данных за границу, создавая стабильную среду для свободного потока данных и формируя «альянс данных». Однако такой подход является ошибочным, и существует риск, что международные соглашения будут признаны недействительными, как, например, соглашения Safe Harbour и Privacy Shield между ЕС и США, которые в итоге были признаны недействительными из-за ограничений ЕС на передачу данных за границу. Тем не менее США будет включать положения о цифровой торговле и потоках данных в соглашения о свободной торговле, а концепция суверенитета данных США будет и дальше продвигаться по всему миру наряду с их политической и экономической деятельностью.

Ситуация в Китае более сложная. С одной стороны, в Китае огромный рынок с населением 1,3 миллиарда человек, объем генерируемых данных чрезвычайно велик, в Китае работает множество иностранных предприятий, поэтому проблема передачи данных за границу может создать угрозу суверенитету и безопасности данных в Китае. С другой стороны, Китай – это быстрорастущая экономика, а цифровая экономика является одним из основных двигателей его экономического развития. В Китае есть такие технологические гиганты, как Huawei, Tencent, Alibaba и ByteDance, а также большое количество иностранных высокотехнологичных компаний, сотрудничающих с китайскими компаниями. Слишком строгие ограничения в сфере трансграничных потоков данных могут ослабить конкурентоспособность национальных компаний на международной арене и снизить уровень выгод от глобализации [10]. Поэтому, если будут установлены более высокие стандарты передачи данных за границу, это негативно скажется на экономическом развитии Китая и международных торговых операциях.

В результате Китай принял политику, направленную на поддержание баланса между киберсуверенитетом и свободными рынками и потоками данных. Чтобы защитить

критически важные данные от потери и способствовать нормальному потоку обычных данных, Китай разработал набор специальных путей для передачи данных за границу, которые в основном включают три вида: оценку безопасности, стандартный контракт и сертификацию защиты [11]. Под оценкой безопасности понимается оценка степени риска посредством административного лицензирования в соответствии с Мерами по оценке безопасности экспорта данных, изданными Государственным управлением интернет-информации. Стандарт или стандартизированный шаблон контракта, подписываемый между экспортерами данных и получателями данных, требует от других стран обеспечить тот же уровень защиты данных, что и в Китае. Эта инициатива ссылается на GDPR ЕС. Сертификация защиты означает получение сертификата от официальной или официально признанной сторонней организации на момент передачи данных за границу о том, что уровень защиты данных получателя сопоставим с китайским.

Однако на практике предусмотренная система управления передачи данных за границу не была реализована. Во-первых, существуют пробелы в регулировании нежизненных и неперсональных данных; существующие законы не обеспечивают полного охвата всех типов данных, а владельцы данных часто предпочитают не декларировать неоднозначные данные, чтобы избежать дополнительной ответственности, которая с ними связана. Во-вторых, отсутствие четких границ между оценками безопасности, стандартными контрактами и сертификатами защиты приводит к пересечению и путанице между режимами. В таких условиях владельцы данных отдают предпочтение более удобной, быстрой и простой сертификации защиты, а эффективность оценки безопасности и стандартных договоров значительно снижается. В-третьих, закон о кибербезопасности предусматривает, что личная информация и важные данные, собранные и сгенерированные, должны храниться в Китае, однако области, на которые он распространяется, конкретно не перечислены [12]. Этот феномен «одного вопроса» широко распространен в процессе управления данными в Китае. В-четвертых, теоретически китайское правительство стремится найти баланс между защитой безопасности сетевых данных и содействием развитию цифровой экономики; однако в процессе реальной работы опасения по поводу безопасности все еще оказывают влияние на соответствующие решения государственных ведомств, предприятий и организаций.

В настоящее время распространение стандартов и систем трансграничной передачи данных в Китае все еще очень ограничено. Важным достижением для Китая на сегодняшний день является подписанное в 2020 году Соглашение о всеобъемлющем региональном экономическом партнерстве (ВРЭП), сторонами которого являются Китай, Япония, Южная Корея, АСЕАН, Австралия и Новая Зеландия. В 2021 году Китай и арабские страны опубликовали Китайско-арабскую инициативу по сотрудничеству в области безопасности данных, которая призывает страны уважать суверенитет данных. Китай также содействует развитию связей с глобальным рынком данных, подавая заявки на членство в признанных международных организациях и международных правилах, таких как Региональное соглашение о всеобъемлющем экономическом партнерстве, Всеобъемлющее и прогрессивное соглашение о Транстихоокеанском партнерстве (CPTTP) и Соглашение о партнерстве в области цифровой экономики (DEPA).

Заключение

Непрерывный поток данных из стран со слабыми цифровыми технологиями в страны-гегемоны может усугубить цифровое неравенство и даже привести к колонизации данных. Поэтому концепция суверенитета данных принимается все большим количеством

стран. ЕС, США и Китай представляют собой три режима выхода из цифрового пространства. В настоящее время ЕС является доминирующим игроком в отстаивании парадигмы суверенитета данных, обладая набором зрелых и практичных механизмов защиты данных. Что касается США, то доминирующее положение в цифровом пространстве заставляет их выступать против барьеров на пути передачи данных и за свободный поток данных, однако США также могут использовать ограничения на передачу данных за границу в качестве оружия геополитической конкуренции. Китай пытается найти средний путь, хотя его нынешний режим выхода из цифрового пространства все еще имеет серьезные недостатки. В целом модель ЕС является достойной моделью для других стран, находящихся в неблагоприятном положении с точки зрения цифровых технологий, а его успехи и установленные стандарты могут позволить снизить стоимость разработки законодательства и правоприменения в других странах. Однако чрезмерные барьеры на пути цифровой мобильности могут также создать подводные камни антиглобализации и ускорить формирование феномена кибербалканизации. Стоит отметить, что между ЕС и США существуют институциональные противоречия по вопросам передачи данных за границу и защиты информации, что приводит к частым конфликтам, которые нередко заканчиваются принятием американскими компаниями штрафных санкций, самый известный пример – серия изменений в требованиях ЕС к продукции Apple. Однако другие страны, не обладающие таким крупным рынком, как ЕС, вряд ли смогут самостоятельно добиться подобных результатов. Геополитизация киберпространства также вызывает тревогу, и в будущем неизбежен рост политического инструментария данных. Как избежать негативного влияния геополитики, особенно в отношениях Китая и США, на глобальную цифровую экономику – вопрос, требующий безотлагательного решения.

Библиография

1. Number of internet and social media users worldwide as of January 2024. https://www.statista.com/statistics/617136/digital-population-worldwide/
2. Digital trust: How to unleash the trillion-dollar opportunity for our global economy. https://www.weforum.org/agenda/2022/08/digital-trust-how-to-unleash-the-trillion-dollar-opportunity-for-our-global-economy/
3. Jones, C.I., Christopher T. (2020). Nonrivalry and the Economics of Data. American Economic Review, 110 (9): 2819-2958.
4. Чэнь Б., Ван Б. Правовое регулирование и совершенствование процедуры вывода данных из Китая в рамках принципа суверенитета данных, Журнал Университета Хуацяо (издание философии и социальных наук), 2024, № 2, С. 49-63. (на китайском языке)
5. General Data Protection Regulation. https://gdpr-info.eu/
6. Восс, У.Г. Трансграничные потоки данных, общий регламент защиты персональных данных и управление данными // Вестник международных организаций: образование, наука, новая экономика. 2022. Т. 17, № 1. С. 56-95. doi: 10.17323/1996-7845-2022-01-03.
7. CLOUD Act Resources. https://www.justice.gov/criminal/cloud-act-resources
8. Лю К.А. Ключевые направления развития наднационального правового регулирования цифрового пространства ЕС на современном этапе // Международное право. 2022. № 1. С.61-75. DOI: 10.25136/2644-5514.2022.1.37674 URL: https://e-notabene.ru/wl/article_37674.html
9. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R1925
10. Сюн Т., Конг С. Построение механизма глобального управления, основанного на

концепции суверенитета данных-вызовы, направления и пути // Журнал региональных и страновых исследований, 2024. № 2. С. 75-90. (на китайском языке)
11. Е Ч., Янь В. О текущей ситуации, проблемах и путях улучшения трансграничной системы передачи данных в Китае // Журнал Пекинского университета аэронавтики и астронавтики (издание по общественным наукам). 2024. № 1. С. 57-71. (на китайском языке)
12. Шелепов, А. В. Подходы стран БРИКС к регулированию данных // Вестник международных организаций: образование, наука, новая экономика. 2022. Т. 17, № 3. С. 212-234. doi: 10.17323/1996-7845-2022-03-0

Результаты процедуры рецензирования статьи

В связи с политикой двойного слепого рецензирования личность рецензента не раскрывается.
Со списком рецензентов издательства можно ознакомиться здесь.

Предметом рецензируемого исследования выступает проблема национального суверенитета цифровых данных и особенности управления трансграничной передачей этих данных в условиях глобальной цифровой экономики. Учитывая бурное развитие цифровой экономики в последние годы, а также опасности, связанные с бесконтрольным оборотом цифровых данных, актуальность выбранной для исследования темы трудно переоценить. К этому можно добавить опасения экспертов по поводу неожиданно возросших возможностей искусственного интеллекта. К сожалению, автор не дал себе труда должным образом отрефлексировать теоретико-методологическую базу собственного исследования, что не могло не отразиться на качестве используемой терминологии (о чём ниже). Но из контекста можно понять, что в процессе исследования применялись исторический и институциональный подходы к анализу нормативной базы управления трансграничными потоками цифровых данных, а также компаративный метод (для изучения основных моделей этого управления) и критический контент анализ (при изучении конкретных нормативных актов). Вполне корректное применение указанных методов позволило автору получить результаты, обладающие признаками научной новизны. Прежде всего, речь идёт о выявленных трёх ключевых моделях (или «режимах») управления трансграничной передачей цифровых данных – китайской, европейской и северо-американской. Любопытно также заключение автора о специфике ценностной базы, на которой формируются выявленные модели, а также его оценки перспектив каждой из моделей. В структурном плане рецензируемая статья также не вызывает серьёзных нареканий: её логика достаточно последовательна и отражает основные аспекты проведённого исследования. В тексте выделены четыре основных раздела: - «Введение», где ставится научная проблема, обосновывается её актуальность, но, к сожалению, игнорируется обязанность декларировать и аргументировать теоретико-методологический выбор; - «Режимы управления и ключевые законы в области трансграничной передачи данных в ЕС, США и КНР», где выделяются и анализируются основные модели управления трансграничной передачей данных; - «Ценностные ориентации и причины принятия законов в области трансграничной передачи данных в ЕС, США и Китае», где анализируются ценностные основания для формирования конкретной модели, а также достоинства и недостатки этих моделей; - «Заключение», где резюмируются итоги проведённого исследования, делаются выводы и намечаются перспективы дальнейших исследований. Стиль рецензируемой статьи научный. В тексте встречается некоторое количество стилистических погрешностей (например, в первом же предложении сочетание «в производстве и жизни людей» звучит достаточно двусмысленно, что с точки зрения научного стиля недопустимо; и

др.), но в целом он написан достаточно грамотно, на хорошем русском языке, с корректным использованием научной терминологии. Правда, некоторые термины вызывают вопросы. Так, буквальный перевод с английского термина "physical world GDP" как «ВВП физического мира» не только выглядит странно (ВВП может иметь экономика, но не сам «физический мир»), но и не корректно – правильнее было бы перевести как «физический мировой ВВП» или по смыслу «мировой ВВП материальной экономики». Другой пример некорректной терминологии: «высокие технологии, такие как большие данные…». Строго говоря, «большие данные» ("big data") сами по себе не являются технологией (это скорее информация), о технологиях может идти речь, когда эти самые «большие данные» тем или иным способом обрабатываются и используются. Тем более, что сам автор ниже утверждает, что данные являются «продуктом цифровых технологий» и составляют «основу для дальнейшего развития цифровых технологий». Что гораздо корректнее, чем называть технологиями сами «большие данные», подменяя понятия. Собственно, утверждение автора о том, что «большие данные, искусственный интеллект, интернет вещей и блокчейн, занимают лидирующие позиции в мире» также вызывает существенные сомнения. Сам автор ссылается на данные Всемирного банка и говорит о том, что вся доля цифровой экономики превысила 15 % мирового ВВП, но это далеко не соответствует «лидирующим позициям». Хотя действительно, РОСТ цифровой экономики в последние десятилетия впечатляет. Но основу нашей жизни до сих пор составляет реальная экономика, но никак не цифровая. Не менее спорным является утверждение автора о том, что «в отличие от традиционных ресурсов, данные… не подлежат потреблению». Если исходить из традиционного определения термина «потребление» как использование продукта в процессе удовлетворения потребностей, то данные вполне подвержены потреблению – при написании данной рецензии были использованы программные средства, необходимые для получения нужного результата. То есть, данные именно потреблялись. Другое дело, что в процессе потребления эти данные не были уничтожены, как это бывает с многими материальными продуктами, но товарное богатство современной экономики далеко не сводится к производству физических товаров – в конце концов, услуги при потреблении тоже не уничтожаются, хотя и укоренены в обычной, самой что ни на есть традиционной экономике. Впрочем, эти и другие терминологические нюансы нельзя считать критичными при оценке общего научного уровня рецензируемого исследования: несмотря на некоторые незначительные огрехи, в целом автор достаточно глубоко разобрался в теме и вполне освоил её терминологическую специфику. Поэтому незначительные терминологические погрешности не стали основанием для отклонения статьи. Библиография насчитывает 12 наименований, в том числе источники на иностранных языках, и в должной мере отражает состояние исследований по проблематике статьи. Апелляция к оппонентам отсутствует в силу отсутствия обоснования теоретико-методологической базы исследования.

ОБЩИЙ ВЫВОД: несмотря на некоторые недостатки, предложенную к рецензированию статью можно квалифицировать в качестве научной работы, отвечающей основным требованиям, предъявляемым к работам подобного рода. Полученные автором результаты будут интересны политологам, социологам, экономистам, специалистам в области государственного управления, мировой политики и международных отношений, а также студентам перечисленных специальностей. Представленный материал соответствует тематике журнала «Право и политика». По результатам рецензирования статья рекомендуется к публикации.