ИСТОРИЯ И ТЕОРИЯ МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ

DOI 10.35775/PSI.2025.72.7.008
УДК 32.327

С.В. ШИТЬКОВ
кандидат юридических наук,
и.о. Ректора Дипломатической академии МИД России,
Проректор по правовым вопросам МГИМО МИД России,
Россия, г. Москва

СУВЕРЕНИТЕТ ДАННЫХ И ИНФРАСТРУКТУРНАЯ СИЛА: РОССИЙСКИЙ ПОДХОД В СРАВНИТЕЛЬНОЙ ПЕРСПЕКТИВЕ

Статья раскрывает российскую модель цифрового суверенитета как сочетание правового регулирования, контроля над цифровой инфраструктурой и внешнеполитических практик. Теоретическая рамка объединяет «практический поворот» в международных отношениях (суверенитет как компетенция, воспроизводимая через рутинные практики – стандартизация, сертификация, тестирование и т.п.), реалистскую концепцию инфраструктурной власти (роль контроля над сетями и данными как носителя суверенитета), институционализм режимной сложности (пересечение кибербезопасности, торговли и прав человека) и конструктивистский анализ норм (противоречие между принципом суверенитета данных и идеологией свободного потока данных). Эмпирическая база включает анализ ключевых российских актов, официальных документов Китая и Индии. Дополнительно учитываются региональный контур ЕАЭС и глобальные процессы.

Показано, что российская модель опирается на суверенизацию инфраструктуры и данных, выстраивая внешнеполитическую повестку вокруг международной информационной безопасности и цифровой автономии союзов. Практические следствия включают укрепление межведомственной координации, развитие национальных платформ, цифровую интеграцию ЕАЭС и участие России в формировании многосторонних норм.

Ключевые слова: *цифровой суверенитет, суверенитет данных, инфраструктурная сила, Российская Федерация.*

Введение. В последние годы российское руководство стремится обеспечить технологическую независимость и контроль над информационным пространством как основу суверенитета [12]. Концепция цифрового суверенитета обрела особую актуальность на фоне геополитической конфронтации с Западом и санкционного давления [9]. Москва является инициатором и «лидером» международной повестки по обеспечению государственного суверенитета в информационном пространстве. Российская дипломатия прилагает значительные усилия

для продвижения принципа суверенной власти государств над национальным сегментом интернета и норм международной информационной безопасности (МИБ) [2]. В этой связи в статье ставятся следующие исследовательские вопросы:

(RQ1) какие практические меры по суверенизации цифровой инфраструктуры и данных реализует Россия;

(RQ2) как эти практики соотносятся с регулятивными режимами в других странах, прежде всего, в США, ЕС, Китае и Индии?

Работа интегрирует «практический поворот» – рассмотрение суверенитета через призму рутин государственной деятельности (стандарты, сертификация, дипломатия технических норм) – с анализом правовых и инфраструктурных решений. Такой междисциплинарный подход позволяет понять не только нормативно-законодательные аспекты, но и то, как через повседневные практики выстраивается цифровой суверенитет государства.

Теоретико-методологические основания. Практический поворот в МО. Современные теории международных отношений все чаще рассматривают суверенитет не как статичную данность, а как динамическую компетенцию, воспроизводимую через практики и рутины государственной деятельности [7. P. 225-258]. В рамках практик суверенитет государства подтверждается на деле – например, посредством дипломатии стандартов и протоколов, государственных закупок ИТ-решений, процедур сертификации и учений по устойчивости сетей. Государство проявляет свою суверенную власть, вводя национальные требования к технологиям и формируя вокруг них коалиции или альянсы. Подобный подход подчеркивает, что суверенитет – это во многом исполняемая компетенция, а не только юридический статус [15. P. 175-196].

Реализм инфраструктурной власти. Майкл Манн вводит понятие инфраструктурной власти – способности государства проникать в общество и реализовывать решения через разветвленную инфраструктуру [16]. В цифровую эпоху контроль над интернет-инфраструктурой, центрами обработки данных, платформами и коммуникационными сетями становится ключевым ресурсом государственной власти. Реализм инфраструктурной власти предполагает, что суверенитет проявляется через возможность государства строить и управлять критическими цифровыми системами – от национальных доменных зон и маршрутизаторов до облачных платформ. Суверенизация инфраструктуры усиливает власть государства на своей территории и снижает уязвимость перед внешним воздействием. Так, Л. ДеНардис отмечает, что правительства неизбежно все активнее вовлекаются в управление интернетом, требуя ответственности и надежности от технологий, поскольку сбои в киберсистемах ведут к рискам в реальном мире [12; 13]. В противовес либеральной концепции глобального интернета, предполагавшей размывание границ, инфраструктурный реализм исходит из того, что государства будут укреплять цифровые границы для защиты своих интересов.

Конструктивизм и конкуренция норм. В глобальном дискурсе столкнулись две конкурирующие нормы: цифровой суверенитет (право государства

контролировать данные и сеть на своей территории) и свободный поток данных (принцип трансграничной открытости информации как условие инноваций и торговли). В последние годы эта либеральная парадигма подвергается критике за то, что на практике «свободный поток» обернулся глобальной экспансией техногигантов и сбором данных, что аналитики ЮНКТАД назвали «колониализмом данных» [21]. Страны, отстаивающие цифровой суверенитет, во многом реагируют на эти дисбалансы, пытаясь восстановить регуляторный контроль и утвердить альтернативные нормы поведения в цифровой среде. Россия, Китай и другие государства, желающие предотвратить доминирование Запада, стремятся сформулировать нормы цифрового суверенитета (например, принцип невмешательства во внутренние цифровые дела, право на национальные сегменты интернета), и продвигают их в международных организациях.

Российская нормативная и институциональная архитектура цифрового суверенитета. Российский подход к цифровому суверенитету оформлен в ряде стратегических документов и законов, которые совместно создают многоуровневую систему защиты национального цифрового пространства. Ключевыми элементами этой архитектуры являются доктринальные установки в сфере информационной безопасности, законодательство о критической инфраструктуре и Рунете, а также государственные программы развития отечественных технологий [4].

Внешнеполитическое измерение: Россия в многосторонних и региональных форматах. Многосторонние инициативы и ООН. Россия последовательно продвигает идею международно-признанных принципов суверенитета в цифровой сфере на площадке Организации Объединенных Наций. Начиная с конца 1990-х, по инициативе РФ Генассамблея ООН принимает резолюции по обеспечению международной информационной безопасности (МИБ). В 2018 г. Россия добилась создания Открытой рабочей группы ООН по безопасности в использовании ИКТ (РГОС) [1]. В рамках OEWG Москва добивается включения в итоговые отчеты принципа суверенного равенства государств применительно к киберпространству. Российские дипломаты аргументируют, что государственный суверенитет и невмешательство должны полноценно действовать и онлайн так же, как офлайн [13]. Уже в итоговых документах Группы правительственных экспертов ООН (GGE) по МИБ было отражено, что государства обладают суверенной властью на формирование национальной политики в области интернета. Это большой дипломатический успех РФ. Параллельно Россия активно выступает за разработку универсальных правил ответственного поведения государств в информационном пространстве, и за заключение глобальной конвенции по кибербезопасности. Таким образом, на многостороннем треке Россия формирует коалиции (включая Китай, страны ОДКБ, ШОС, и ряд государств Глобального Юга) для продвижения повестки цифрового суверенитета и международно-правового закрепления норм ИКТ-безопасности [10].

Региональная интеграция ЕАЭС-2025. Евразийский экономический союз служит для России площадкой международного сотрудничества. Основные

направления цифровой повестки ЕАЭС до 2025 года, утвержденные решением Высшего Евразийского совета № 12 (11.10.2017), нацелены на формирование общих цифровых инфраструктур союза. Предусмотрено создание интегрированных платформ обмена данными, совместимых стандартов и правовых механизмов, позволяющих странам ЕАЭС совместно отстаивать цифровой суверенитет в отношении внешних игроков. Например, реализуется проект системы цифровой прослеживаемости товаров во всем ЕАЭС к 2025 г., который позволит отслеживать перемещение импортных и взаимных товаров по единым правилам. Это повышает прозрачность торговли и препятствует санкционным рискам, одновременно создавая единую инфраструктуру доверия между участниками союза. Другая инициатива – интегрированная информационная система ЕАЭС (ИИС), объединяющая национальные сегменты для обмена таможенными, финансовыми и иными данными. Уже сейчас действует механизм обмена сведениями о перевозках, запущены пилоты по взаимному признанию электронных документов. Все эти проекты закрепляют лидерство России как основного разработчика и донора технологий в ЕАЭС [4]. С одной стороны, плюсы для союзников – доступ к современным цифровым инструментам (напр., системы маркировки товаров, интероперабельность госуслуг), экономия на масштабах и повышение безопасности (общие стандарты облегчают киберзащиту). Аналитики ВБ отмечают, что реализация совместной цифровой повестки даст всем странам ЕАЭС синергетический эффект: рост экономики до +1% ВВП в год к 2025 за счет цифровизации торговли и управления. Региональный сегмент суверенизации включает также союз ОДКБ (в части киберучений и обмена данными) и Союзное государство с Беларусью (где формируется единое цифровое пространство). В итоге, на региональном уровне Россия стремится выстроить блок цифровых альянсов, способных совместно отстаивать свои правила в глобальной цифровой экономике [16].

Сравнительный анализ режимов цифрового суверенитета. США традиционно провозглашают приверженность идее открытого интернета, но де-факто выстроили режим, в котором первостепенное значение имеет нацбезопасность и глобальный доступ к данным для разведсообщества [5]. Ключевой элемент – секция 702 закона FISA, дающая Агентству национальной безопасности (АНБ) право получать из иностранных источников данные переписки нерезидентов без ордера. В апреле 2024 года, после бурных дебатов, Конгресс продлил действие параграфа 702 еще на 2 года, одновременно расширив возможности государства по принудительному сотрудничеству частных компаний. В новую редакцию вошло уточненное определение «поставщика электронных коммуникационных услуг» (ECSP), под которое теперь подпадают любые сервис-провайдеры, имеющие доступ к оборудованию, используемому для передачи или хранения данных. Это изменение, по сути, позволяет властям требовать данные не только от классических телекомов и облачных корпораций, но и от более широкого круга структур (например, операторов дата-центров). Правозащитники встревожены экстерриториальностью этой нормы – правительство США усилило

юридические рычаги получения данных, хранящихся за рубежом, через американских провайдеров [14].

Другим инструментом экстерриториального охвата стал принятый в 2018 г. CLOUD Act. Он прямо разрешил американским правоохранительным органам предъявлять ордера на данные компаниям, зарегистрированным в США, независимо от места физического хранения информации. Тем не менее, CLOUD Act закрепляет глобальную юрисдикцию США в цифровой сфере.

В противоположность подходу «суверенного интернета», американская модель уповает не на национальную сегментацию сети, а на проекцию своей правовой системы вовне, фактически ставит под вопрос цифровой суверенитет других стран.

Суверенитет в американском понимании – это возможность проецировать свои законы вовне, даже в ущерб суверенитету других (что критики называют «цифровым неоколониализмом» [10]). Примечательно, что при всей риторике свободы интернета, США не колеблясь вводят санкции и технологические ограничения против стран-конкурентов (запреты на экспорт чипов в США, отключение от платформ), тем самым де-факто расчленяя глобальную сеть ради геополитических целей. Это показывает, что глобалистская модель США трансформируется под влиянием реалий конкуренции великих держав, и цифровой суверенитет США приобретает форму укрепления собственной технологической гегемонии.

Европейский союз: «эффект Брюсселя» и регуляторная экстерналия. Европейский союз выстроил уникальную регуляторную модель цифрового пространства, основанную на ценностях приватности, киберустойчивости и потребительских правах. Через эту модель ЕС оказывает глобальное влияние, феномен которого получил название «эффект Брюсселя» – когда европейские нормы распространяются по всему миру [9]. Центральным столпом является Общий регламент по защите данных (GDPR) – всеобъемлющий закон о персональных данных. GDPR установил жесткие требования к сбору и обработке персональных данных (принцип согласия, минимизации, права субъектов), большие штрафы за нарушения (до 4% оборота) и экстерриториальное применение: он действует в отношении любых компаний, работающих с данными жителей ЕС, даже если они вне Европы. За несколько лет GDPR стал де-факто глобальным стандартом приватности – многие страны (Бразилия, ЮАР, Индия частично) приняли аналогичные законы, а транснациональные корпорации внедрили единые политики, совместимые с GDPR [20]. Таким образом, ЕС сумел превратить законодательство в рычаг проекции нормативной силы: компании предпочитают унифицировать стандарты под строгие европейские, нежели поддерживать разные уровни требований для разных стран [11].

Акт об искусственном интеллекте (AI Act) –первый в мире комплексный закон об ИИ, политически согласованный в 2023 г. и вступающий в силу поэтапно с 2024-2026 гг. AI Act использует риск-ориентированную модель регулирования: все приложения ИИ делятся на четыре категории риска. Недопустимый риск – ИИ,

противоречащий ценностям (например, социальный рейтинг граждан по китайскому образцу, или распознавание эмоций в полиции) – такие системы будут прямо запрещены. Высокий риск – сюда попадают ИИ-системы для критических сфер (безопасность, правосудие, биометрическая идентификация в публичных местах и т.п.) – их можно использовать, но только при соблюдении жестких требований: регистрация в спецреестре, оценка соответствия, документация, обеспечение человеческого надзора и качества датасетов [7]. Ограниченный риск – ИИ, требующий минимум прозрачности (например, chatbots должны помечать себя как машины). Минимальный риск – большинство потребительских приложений ИИ, на них регулирование не накладывается.

Модель ЕС – «нормативная сила» с выраженным регуляторным экстерналитетом [18]. Суверенитет данных здесь понимается прежде всего как суверенитет личности (защита прав индивидуума на свои данные) и «стратегическая автономия» союза (уменьшение зависимости от внешних технoплатформ). ЕС делает ставку на силу права: устанавливая строгие нормы у себя, ЕС фактически навязывает их иностранным компаниям, создает глобальные прецеденты. Это мягкая форма цифрового суверенитета. Сейчас, когда идет конкуренция технoблоков, эффективность «эффекта Брюсселя» в новых сферах (например, ИИ) будет проверяться: смогут ли правила ЕС превалировать, или другие центры (США, Китай) предложат альтернативы?

Китай: «комплексная суверенизация данных». Китайская Народная Республика выстроила наиболее целостный и жесткий режим государственного контроля над цифровым пространством, часто упоминаемый как модель «киберсуверенитета». Он основывается на трех фундаментальных законах, принятых в 2017-2021 гг.: Закон о кибербезопасности (CSL, вступил в силу июнь 2017), Закон о безопасности данных (DSL, сентябрь 2021) и Закон о защите персональной информации (PIPL, ноябрь 2021). В совокупности они создают комплексную систему регулирования всех типов данных – от личных до промышленных.

Китай одним из первых в мире ввел законодательно локализацию данных, мотивируя это защитой суверенитета и национальной безопасности. Кроме того, CSL усилил требования к контентной цензуре (Great Firewall), кибербезопасности компаний (сертификация оборудования, контроль телеком-оборудования) и дал властям полномочия отключать сети в чрезвычайных ситуациях. CSL также обладает экстерриториальной статьей – распространяется на действия за рубежом, если они наносят вред китайской КИИ или публике (хотя механизм привлечения иностранных нарушителей не вполне определен) [3. С. 38-51].

Законодательство КНР требует локализации – операторы критической инфраструктуры и крупные сборщики данных обязаны хранить все личные данные в Китае. Иными словами, Китай установил зеркальный по отношению к ЕС принцип экстерриториальности: если иностранная фирма хочет китайский рынок, она должна соблюдать китайские правила по данным.

Китайская модель суверенизации данных опирается также на мощную техно-инфраструктуру, построенную за десятилетия. «Великий китайский

файрвол» – наглядное проявление киберсуверенитета, работающее с конца 1990-х [11. P. 107-145]. Параллельно выросли национальные IT-гиганты (Baidu, Alibaba, Tencent, Huawei), которые стали своеобразными «стратегическими агентами» государства: с одной стороны, частные корпорации, с другой – тесно сотрудничающие с властями по вопросам данных и инфраструктуры (например, Huawei – лидер в национальных 5G-сетях). КНР активно развивает и экспортирует технологии суверенного интернета: от систем видеонаблюдения с ИИ до платформ электронной коммерции.

Таким образом, китайская модель – «тотальная суверенизация», охватывающая инфраструктуру, потоки данных и контент. При этом Китай участвует в глобальной цифровой экономике [3. С. 38-51].

Индия: «суверенитет развития». Индия также склоняется к модели суверенного контроля над данными – однако с упором на стимулирование собственной цифровой экономики. В августе 2023 г. Индия приняла Закон о цифровой персональной информации (Digital Personal Data Protection Act, DPDP 2023) – первую полноформатную реформу в этой сфере за 10+ лет обсуждений. Он фокусируется только на цифровых персональных данных, не вводя сложных категорий вроде «чувствительные данные» (все типы данных регулируются единообразно). DPDP Act основан на принципах согласия и ограниченности (требуется явное согласие, сбор лишь необходимых данных), но при этом дает правительству широкие полномочия делать исключения: например, освобождать государственные агентства от соблюдения некоторых требований ради «суверенитета и общественного порядка». Такой поэтапный подход показывает прагматизм: Индия стремится избежать шока для индустрии IT-аутсорсинга (одной из ведущих в мире), давая компаниям время адаптироваться.

Индийский режим цифрового суверенитета можно охарактеризовать как «балансирование между развитием и контролем». Дели продвигает концепцию свободного потока данных с доверием на международных форумах, подчеркивая, что данные нужны для развития инноваций и экономики. При этом Индия ужесточила национальные правила. Введены требования локализации для определенных данных: например, платежные данные граждан должны храниться только в Индии (правило Резервного банка 2018 г.). Дух закона – дать индийскому правительству инструмент контролировать трансграничные потоки при необходимости. Также Индия активно выстраивает свою цифровую инфраструктуру: проекты India Stack (набор открытых API для цифровой идентичности, платежей, документов) создали уникальную экосистему, управляемую государством (например, система идентификации Aadhaar покрывает свыше миллиарда людей и является основой получения услуг). Эти решения Индия теперь экспортирует – ряд стран Юга перенимают India Stack, что повышает цифровое влияние Дели.

Таким образом, индийская модель – «суверенитет через развитие». Индия хочет быть крупным цифровым хабом, делает упор на построение национальных мощностей (крупнейшие в мире по охвату гос. цифровые сервисы), точечное

регулирование (ограничение нежелательных иностранных приложений в целях защиты данных граждан) и постепенное внедрение всеобъемлющего закона о данных. Индия поддерживает суверенное право государств на регулирование, но и выступает за интероперабельность и глобальные стандарты. В конечном счете, индийский цифровой суверенитет – это суверенитет восходящей державы, которая желает обезопасить свой киберпространство, не пожертвовав выгодами глобальной интеграции.

Дискуссия: место России. Российская модель сочетает элементы жесткого и умеренного суверенитета и является гибридной [6. С. 33-51]. С одной стороны, приняты меры по защите инфраструктуры, что придает российскому киберпространству черты автономной экосистемы. В 2015 г. введена локализация персональных данных, но без тотального контроля над бизнес-данными как в Китае. То есть регуляторный режим селективный: государство усиливает контроль там, где видит угрозу безопасности, но не ограничивает и поддерживает частный ИТ-сектор. Однако с 2022-2023 удаляются пробелы в регулировании (новые требования по большим данным, регулирование иностранных мессенджеров и VPN, законопроекты о налогах на иностранные ИТ-услуги и т.д.).

Таким образом, российскую модель отличает акцент на инфраструктурном суверенитете: контроль над маршрутами трафика, своими ЦОДами, средствами шифрования, программным обеспечением – нацеленным на замену западных сервисов отечественными (RuStore вместо Google Play, СмартВижн вместо Zoom и т.п.). Данные рассматриваются как стратегический ресурс: все операторы КИИ и органы должны хранить их внутри, использовать российские СУБД и облака.

ЕАЭС подкрепляет способность России экспортировать свою модель, реализуя цифровую интеграцию на постсоветском пространстве, Москва закрепляет российские стандарты (в криптографии, в системах прослеживаемости и т.д.) как региональные. Это подтверждает гипотезу о «регуляторном экспорте через союзы». Например, соглашения ЕАЭС предусматривают взаимное признание российских требований по сертификации IT-продукции, что облегчает их принятие партнерами. В условиях геополитического раскола российская цифровая зона влияния включает страны СНГ, БРИКС.

В целом, Россия стремится занять место лидера цифровой коалиции незападных стран «мирового большинства» – наряду с Китаем и Индией – противопоставив ее западноцентричному порядку. При этом российская модель еще эволюционирует: изначально умеренно-селективная, под влиянием конфликта с Западом она сдвигается к более жесткой. Россия уже сейчас заявляет о намерении строить «новый цифровой порядок» на основе суверенитета, вместе с партнерами по БРИКС [3. С. 38-51]. Российская модель цифрового суверенитета ориентирована проактивное формирование собственного цифрового порядка. Она не сводится к изоляции – скорее это стратегия управляемой интероперабельности: Россия стремится интегрироваться в мировое киберпространство на основании национальных интересов, сохраняя суверенитет в области инфраструктуры и данных. Внешнеполитически Москва делает ставку на нормотворчество

в сфере международной информационной безопасности и институционализацию региональных цифровых блоков как противовес доминированию западных техногигантов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. **Бухарин В.В.** Компоненты цифрового суверенитета России // Вестник МГИМО-Университета. 2016.
2. **Зиновьева Е.С.** Международная информационная безопасность: проблемы многостороннего и двустороннего сотрудничества. М.: МГИМО, 2021.
3. **Зиновьева Е.С., Шитьков С.В.** Цифровой суверенитет в практике международных отношений // Международная жизнь. 2023. № 3.
4. **Попова И.М.** Проблемы реализации цифровой повестки ЕАЭС // Вестник международных организаций. 2021.
5. **Ребро О.В.** Категория «цифрового суверенитета» // Международные процессы. 2021.
6. **Шитьков С.В.** Концептуальные основания анализа цифрового суверенитета в современной мировой политике // Международная жизнь. 2025. № 2 (44).
7. **Bigo D.** Pierre Bourdieu and international relations: Power of practices, practices of power // International political sociology. 2011. Vol. 5. No. 3.
8. **Belli L. (ed.).** CyberBRICS: Cybersecurity regulations in the BRICS countries. Springer Nature, 2021.
9. **Bradford A.** The Brussels Effect: How the European Union Rules the World. Oxford UP, 2020.
10. **Couldry N., Mejias U.** The Costs of Connection: How Data Is Colonizing Human Life and Appropriating It for Capitalism. Stanford UP, 2019.
11. **Creemers R.** China's conception of cyber sovereignty // Governing cyberspace: Behavior, power and diplomacy. 2020.
12. **DeNardis L.** The Internet in Everything: Freedom and Security in a World with No Off Switch. Yale University Press, 2020.
13. **DeNardis L.** The Global War for Internet Governance. Yale UP, 2014.
14. **Jessop B.** State Theory: Putting the Capitalist State in Its Place. Cambridge: Polity Press, 1990.
15. **Kustermans J.** Parsing the practice turn: Practice, practical knowledge, practices // Millennium. 2016. Vol. 44. No. 2.
16. **Mann M.** Infrastructural power revisited // Studies in comparative international development. 2008. Vol. 43. No. 3.
17. **Pierucci F.** Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace // Digital Society. 2025. Vol. 4. No. 1.
18. **Sassen S.** Territory, Authority, Rights: From Medieval to Global Assemblages. Princeton: Princeton University Press, 2006.
19. **Srnicek N.** Platform Capitalism. Polity, 2017.

20. The Role of African Governments and Multilateral Organizations in Increasing the Footprints of Multi-Tenant Data Centres and Cloud Infrastructure in Africa // Smart Africa, March 15, 2022 // https://smartafrica.org/the-role-of-african-governments-and-multilateral-organizations-in-increasing-the-footprints-of-multi-tenant-data-centres-and-cloud-infrastructure-in-africa/#:~:text=A%20closer%20look%20at%20Africa,is%20hosted%20outside%20the%20continent.
21. UNCATD Digital Economy Report 2021 // https://unctad.org/page/digital-economy-report-2021.

S.V. SHITKOV
Candidate of Juridical Sciences,
Acting Rector, Diplomatic Academy of the Ministry of Foreign Affairs of the Russian Federation, Vice Rector for Legal Affairs, MGIMO University, Moscow, Russia

DATA SOVEREIGNTY AND INFRASTRUCTURE POWER: THE RUSSIAN APPROACH IN COMPARATIVE PERSPECTIVE

The article examines the Russian model of digital sovereignty as a combination of legal regulation, control over digital infrastructure, and foreign policy practices. The theoretical framework integrates the «practice turn» in international relations (sovereignty as a competency reproduced through routine practices – standardization, certification, testing, etc.), the realist concept of infrastructural power (the role of control over networks and data as a carrier of sovereignty), institutionalism of regime complexity (the intersection of cybersecurity, trade, and human rights), and constructivist analysis of norms (the contradiction between the principle of data sovereignty and the ideology of free data flow). The empirical basis includes an analysis of key Russian legislative acts, official documents from China and India. Additionally, the regional context of the EAEU and global processes are taken into account.

It is demonstrated that the Russian model relies on the «sovereignization» of infrastructure and data, shaping its foreign policy agenda around international information security and the digital autonomy of alliances. Practical implications include strengthened interagency coordination, the development of national platforms, digital integration within the EAEU, and Russia's participation in shaping multilateral norms.

Key words: *digital sovereignty, data sovereignty, infrastructural power, Russian Federation.*