# ТЕОРИЯ И ИСТОРИЯ МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ

**DOI 10.35775/PSI.2025.120.8.017**
**УДК 32**

**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

*В статье исследуется российская концепция цифрового суверенитета как совокупность правовых, институциональных и инфраструктурных практик, обеспечивающих контроль над данными, сетью и критическими цифровыми системами. Развивается интегральный подход, сочетающий «практический поворот» в теории международных отношений, реалистское понимание инфраструктурной власти, анализ сложных режимов цифрового управления и конструктивистский взгляд на нормативные конфликты. Эмпирическая основа включает анализ ключевых российских законов и стратегий, сравнительный обзор американского, европейского, китайского и индийского регулирования, а также оценку региональных (ЕАЭС) и глобальных процессов. Показано, что российская модель формируется на стыке безопасности и развития, опираясь на суверенную инфраструктуру и участие в международной нормотворческой деятельности.*

***Ключевые слова:*** *цифровой суверенитет, практический поворот, цифровизация, интегральный подход, реалистское понимание, цифровое управление, конструктивистский взгляд, США, ЕС, Китай, Индия.*

В начале двадцать первого века технологии связи, данные и облачные платформы стали критически важным ресурсом государств и корпораций. На этом фоне в российском политическом дискурсе утверждается идея «цифрового суверенитета» [1. С. 30-49]. Под ней понимают способность государства самостоятельно определять политику в области информационной инфраструктуры, контролировать национальный сегмент интернета, защищать данные граждан и собственные платформы от внешнего влияния. Поворот к суверенизации цифровой сферы усилился после геополитических кризисов и санкций, обострivших вопрос технологической зависимости и уязвимости. Скандалы вокруг глобального надзора, инициированные разоблачениями Эдварда Сноудена, подорвали

доверие к транснациональным сервисам и стимулировали поиски альтернативных моделей управления сетью [8; 13].

Россия позиционирует себя инициатором международной дискуссии о суверенитете данных. На площадках ООН и других форумов российская дипломатия последовательно продвигает принципы суверенной юрисдикции государств и норм международной информационной безопасности [6. P. 707-732; 15]. Внутренняя политика акцентирует развитие отечественных технологий, импортозамещение в критических сегментах, создание собственных сетевых сервисов и платформ [3]. Данная статья ставит две взаимосвязанные исследовательские задачи: во-первых, описать, какие конкретные правовые и институциональные меры реализует Россия для суверенизации цифровой среды; во-вторых, показать, как эти практики соотносятся с регулированием в ведущих центрах силы – США, Европейском союзе, Китае и Индии, а также с региональной интеграцией в рамках Евразийского экономического союза [3; 15].

Для решения этих задач выбран междисциплинарный подход. Он соединяет политико-юридический анализ российских документов, теории практик (practice turn), выделяющие роль рутинных действий и стандартов, концепцию инфраструктурной силы М. Манна, согласно которой государство проявляет власть, контролируя сети и инфраструктуру, и институциональную теорию, рассматривающую взаимодействие различных режимов (безопасности, торговли, прав человека) вокруг данных. Также учитывается конструктивистский аргумент о столкновении двух норм: суверенитета данных и свободного потока информации. Российский опыт помещается в сравнительный контекст, что позволяет выявить общие тенденции и специфику.

**Теоретико-методологические основания.** Современные дискуссии о суверенитете уходят от его классического понимания как статуса государства в международном праве. В рамках «практического поворота» исследователи рассматривают суверенитет как динамическую компетенцию, которая подтверждается через повторяющиеся действия. Государственные органы задают правила игры, внедряют стандарты, проводят сертификацию, тренировки устойчивости сетей, закупают отечественное оборудование [9; 10. P. 239-260]. Суверенитет в этой логике – это не просто юридический атрибут, а совокупность практик, обеспечивающих способность диктовать условия развития и эксплуатации инфраструктуры. Применительно к цифровой сфере это выражается в установлении требований к технологиям, данным и связям, а также в построении коалиций вокруг этих требований.

Суверенитет неразрывно связан с властью над инфраструктурой. Согласно концепции инфраструктурной силы, предложенной социологом Майклом Манном, государство контролирует общество через управление материальными и информационными сетями [11]. В условиях цифровой эпохи интернет, дата-центры, спутниковая связь, облачные сервисы становятся критическими каналами. Способность государства вмешиваться в их работу – ограничивать трафик, фильтровать информацию, настаивать на локализации данных, – превращается

в форму власти, сопоставимую с военной или экономической мощью. Осознание этого переводит акцент с абстрактных свобод на конкретные механизмы контроля над сетями.

**Нормативно-институциональная архитектура России.** Российская политика в области цифрового суверенитета опирается на набор стратегических документов и законов. Ключевой рамочный акт – Доктрина информационной безопасности 2016 года [3]. В ней впервые закреплено, что рост зависимости от иностранных ИКТ несет угрозу национальной безопасности. Доктрина призывает развивать собственную микроэлектронику, программное обеспечение и средства защиты информации, а также продвигать на международной арене нормы, гарантирующие суверенное право государств управлять национальными сегментами сети. Это было продолжено в Стратегии национальной безопасности-2021, где достижения технологической и цифровой независимости названы одной из приоритетных задач. Стратегия подчеркивает угрозу вмешательства через информационные каналы и необходимость защиты критической инфраструктуры, призывая снизить зависимость от иностранных поставщиков и стимулировать разработку отечественных аналогов.

Главным правовым механизмом стала Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры» (2017) [9]. Он определил категории значимых объектов КИИ (госорганы, энергокомпании, финансовые и медицинские учреждения), ввел обязательные меры киберзащиты и регулярный аудит, обязал операторов подключаться к государственной системе обнаружения и предупреждения атак (ГосСОПКА). Значимые операторы должны хранить и обрабатывать данные на территории России, использовать сертифицированные средства защиты и сообщать властям обо всех инцидентах. В 2025 году вступят поправки, усиливающие требование перехода на российское ПО и оборудование. Закон институционализировал представление о том, что государство не только может, но и обязано регулировать цифровые системы, обеспечивая общественную безопасность. Российские компании восприняли эти требования неоднозначно: крупные игроки получили стимул развивать отечественные решения, а малый бизнес ощутил рост нагрузки.

Другой вехой стала разработка закона № 90-ФЗ (2019) о «суверенном интернете». Он предусмотрел создание национальной системы маршрутизации и доменных имен, обязательную установку оборудования глубокого анализа пакетов (DPI) на сетях операторов и возможность автономной работы российского сегмента при угрозе отключения от глобальной сети. По задумке, система должна защитить интернет-каналы от внешних воздействий и фильтровать трафик, исключая запрещенный контент. Критики усматривают в этой практике риски цензуры и надзора, однако власти отмечают необходимость готовности к кибератакам и внешним отключениям. Закон также распространил требование локализации баз данных на иностранные сервисы, работающие в России: компании должны хранить персональные данные граждан на российских серверах, а в случае отказа грозит замедление трафика или блокировка,

как произошло с LinkedIn. Поправки 2023 г. ужесточили ответственность и ввели крупные штрафы за несоблюдение требований.

Политика в области искусственного интеллекта (Указ Президента № 490, 2019) подчеркивает, что ИИ рассматривается как стратегический ресурс суверенитета [10]. Национальная стратегия ставит цели догнать мировых лидеров по алгоритмам и вычислениям, развивать отечественную элементную базу, кадры и исследования. Приоритетом обозначена безопасность: ИИ должен использоваться этично, с защитой прав человека, прозрачностью и предотвращением манипуляций. Российский подход предполагает гибкость: вместо жесткой как у ЕС регламентации рисков внедрен Кодекс этики ИИ и разработаны свыше сотни ГОСТов для ИИ-систем. Обновления 2023-2024 гг. делают акцент на практическом внедрении в государственное управление и создание собственных больших языковых моделей. ИИ-политика показывает стремление сочетать развитие инноваций с укреплением технологического суверенитета, избегая жестких барьеров, которые могут тормозить бизнес.

**Сравнительный анализ цифровых режимов.**

**Соединенные Штаты.** США декларируют приверженность открытой сети, но фактически выстраивают модель, основанную на национальной безопасности и экстерриториальных правовых инструментах. Секция 702 Закона о надзоре в целях внешней разведки (FISA) позволяет Агентству национальной безопасности получать данные о переписке нерезидентов без ордера. В 2024 г. Конгресс продлил действие § 702 и расширил определение поставщиков услуг, что обязывает отдавать данные даже операторов дата-центров и облачных сервисов. CLOUD Act 2018 г. позволяет американским властям требовать данные у компаний, независимо от места их хранения, и заключать двусторонние соглашения об обмене такими данными. Экстерриториальный характер этих законов приводит к тому, что Соединенные Штаты фактически претендуют на юрисдикцию над глобальными потоками данных. При этом США распространяют свои стандарты кибербезопасности (например, NIST CSF 2.0), побуждая партнеров добровольно следовать им. Такой подход сочетает риторику свободного интернета с практикой глобального контроля.

**Европейский союз.** Европейский союз выработал уникальную нормативную модель, основанную на защите прав граждан. GDPR (2018) установил строгие требования к обработке персональных данных, экстерриториально распространяется на компании по всему миру и предусматривает крупные штрафы. Директива NIS2 (2022) расширила круг субъектов, обязанных соблюдать требования кибербезопасности, и ввела обязанность оценивать риски в цепочках поставок. Регламент о данных (Data Act, 2023) закрепил права пользователей на доступ к данным, запретил навязывание несправедливых условий и обязал провайдеров обеспечивать переносимость данных. Акт об искусственном интеллекте (AI Act) классифицирует ИИ-системы по риску и вводит ограничения на высокорисковые приложения (например, биометрический контроль), дополняя правила GDPR. Совокупность этих актов формирует тип «регуляторного экстернализма»,

поскольку компании во всем мире вынуждены соответствовать европейским правилам, чтобы работать на рынке ЕС. Европейский подход рассматривает цифровой суверенитет как обеспечение прав личности и стратегической автономии, не прибегая к цензуре или локализации контента, но усиливая контроль над технологиями. Вместе с тем Брюссель стремится уменьшить зависимость от иностранных технологий, развивая инициативы GAIA-X и другие европейские облака.

**Китай.** Китайская Народная Республика построила наиболее жесткую модель киберсуверенитета [6; 15. P. 707-732]. Законы о кибербезопасности (2017), безопасности данных (2021) и защите персональной информации (2021) вводят строгие требования локализации данных, государственное лицензирование всех операторов критической инфраструктуры, классификацию данных по уровню важности и обязательные проверки безопасности при передаче информации за рубеж. Китайский подход сочетает масштабную инфраструктурную автономию (в том числе «Великий китайский файрвол», национальные поисковики и соцсети) с жесткой цензурой. Иностранные сервисы допускаются на рынок только при условии полного соответствия правилам цензуры и предоставления доступа к данным властям. Вместе с тем Китай активно развивает национальных технологических гигантов (Alibaba, Tencent, Huawei) и экспортирует свои решения в развивающиеся страны. Эта модель обеспечивает почти полный контроль государства над информационной средой, но вызывает опасения по поводу свободы выражения и инноваций. В международной дипломатии Китай совместно с Россией продвигает концепцию «киберсуверенитета» и добивается признания права государств регулировать свой интернет.

**Индия.** Индия формирует собственный подход, ориентированный на баланс между развитием и контролем [14. P. 123-140]. Закон о цифровой персональной информации (Digital Personal Data Protection Act, 2023) стал компромиссом между потребностями быстро растущего ИТ-сектора и требованиями безопасности. Он основывается на принципе согласия, ограничивает объем собираемых данных и допускает исключения для государственных нужд. Первоначальные планы жесткой локализации были смягчены: правительство будет определять страны, куда разрешен экспорт данных. Индия также развивает уникальную цифровую инфраструктуру – «India Stack» с открытыми API, системой идентификации Aadhaar и платформой цифровых платежей, – которая способствует инновациям и экспортируется в страны Глобального Юга. В то же время Нью-Дели периодически блокирует иностранные приложения, считая их угрозой безопасности. Индийский режим можно охарактеризовать как прагматичный: стремление сохранить открытость для бизнеса сочетается с готовностью к точечным ограничениям.

**Типология и место России.** Сравнение позволяет выделить три типовых модели цифрового суверенитета. «Жесткая» модель (Китай) предполагает полный государственный контроль, строгую локализацию данных и цензуру. «Нормативная» модель (ЕС) акцентирует права граждан и устанавливает

правила для частных компаний без изоляции инфраструктуры. «Селективная» модель (Индия) комбинирует стремление к развитию с точечным контролем. Российский подход занимает промежуточное положение и может быть охарактеризован как «инфраструктурно-правовая суверенизация» [3]. С одной стороны, Москва принимает жесткие меры на инфраструктурном уровне: требует локализации данных, создает автономный сегмент сети, строит национальные платформы и облака. С другой стороны, российское законодательство о персональных данных менее строго, чем европейское, и не исключает участия иностранных компаний. Россия унаследовала элементы китайской модели (контроль над трафиком, DPI, локализация), но стремится сохранить некоторую открытость для бизнеса и развития. В условиях санкций тренд движется к усилению самоопоры; при этом Россия ищет союзников, чтобы сформировать «союз суверенных сегментов» и предъявить альтернативу западному порядку.

**Заключение.** Российский цифровой суверенитет эволюционирует от оборонительной реакции на внешние угрозы к проактивному формированию собственной цифровой экосистемы и международной повестки. Это стратегия «управляемой интероперабельности»: стремление интегрироваться в мировой киберпространство на собственных условиях, контролируя критические слои и защищая данные. Российская модель сочетает правовые акты, развитие инфраструктуры, внутренние практики и внешнюю дипломатию. По сравнению с китайской она менее тотальна, по сравнению с европейской – более сосредоточена на безопасности государства, по сравнению с индийской – больше акцентирует импортозамещение и защиту критической инфраструктуры.

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. **Дудин М.Н., Шкодинский С.В., Усманов Д.И.** Цифровой суверенитет России: барьеры и новые траектории развития // Проблемы рыночной экономики. 2021. № 2 // http://www.market-economy.ru/archive/2021-02/2021-02-030-049-dudin.pdf.
2. **Barbesino K.** Treatment and Evolution of Digital Rights: A Comparative Analysis of China, Russia, the United States, and Germany. Rollins College, 2019 // https://scholarship.rollins.edu/honors/97/.
3. **Belli L., Gaspar W.B., Jaswant S.S.** Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries // Computer Law & Security Review. 2024. DOI: 10.1016/j.clsr.2024.105794.
4. **Coche E., Kolk A., Ocelík V.** Unravelling cross-country regulatory intricacies of data governance: the relevance of legal insights for digitalization and international business // Journal of International Business Policy. 2024 // https://link.springer.com/article/10.1057/s42214-023-00172-1.
5. **Dzigal N., Safarpour D., Godolja D., Süsslin L.** Digital Sovereignty and Geopolitics in the Field of Data Protection: A Comparison of the EU, China, and the USA. 2025 // https://www.researchgate.net/publication/389356939.

6. **Gao R.Y.** A Battle of the Big Three? Competing Conceptualizations of Personal Data Shaping Transnational Data Flows // Chinese Journal of International Law. 2023. Vol. 22. No. 4. DOI: 10.1093/chinesejil/jmad040.
7. **Gur B.A.** Cybersecurity, European digital sovereignty and the 5G rollout crisis // Computer Law & Security Review. 2022. Vol. 46. DOI: 10.1016/j.clsr.2022.105679.
8. **Kokas A.** Trafficking Data: How China is Winning the Battle for Digital Sovereignty. New Haven: Yale University Press, 2023.
9. **Li Y.** Cross-Border Data Transfer Regulation: A Comparative Study of China and Europe. University of Macerata, 2021 // https://u-pad.unimc.it/handle/11393/283978.
10. **Malone M.** Data Localization, Hegemony, and the Popular Will: A View from Canada // In: Comparative Data Law: The Munich Global Data Law Project. Cambridge: Cambridge University Press, 2025. DOI: 10.1017/9781009531139.
11. **Mann M.** The Sources of Social Power. Vol. 1: A History of Power from the Beginning to A.D. 1760. Cambridge: Cambridge University Press, 1986.
12. **Olorunlana T.J.** The US Role in Shaping Global Cybersecurity Norms // International Journal of Science, Arts, Technology & Education (IJSATE). 2025. Vol. 1. No. 4 // https://ijsate.com/wp-content/uploads/2025/07/V1I4P7_IJSATE032537.pdf.
13. **Taylor R.D.** Sovereignty and Trans-Border Data Flows: The Debate over Data Localization. ResearchGate, 2019 // https://www.researchgate.net/publication/356613541.
14. **Vedika.** Digital Sovereignty and India's Data Dilemma // Jus Corpus Law Journal. 2024. Vol. 5. No. 1 // https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/juscrp5&section=116.
15. **Yun H.** China's Data Sovereignty and Security: Implications for Global Digital Borders and Governance // Chinese Political Science Review. 2025. Vol. 10. No. 2. DOI: 10.1007/s41111-024-00269-9.

**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 A COMPARATIVE PERSPECTIVE

*This article examines the Russian concept of digital sovereignty as a set of legal, institutional, and infrastructural practices that ensure control over data, networks, and critical digital systems. It develops an integrated approach that combines the «practical turn» in international relations theory, a realist understanding of infrastructural power, an analysis of complex digital governance regimes, and a constructivist perspective on normative conflicts. The empirical framework includes an analysis of key Russian laws and strategies, a comparative review of American, European, Chinese, and Indian regulation, and an assessment of regional (EAEU) and global processes. It is shown that the Russian model is being formed at the intersection of security and development, relying on sovereign infrastructure and participation in international norm-setting activities.*

***Key words:*** *digital sovereignty, practical turn, digitalization, integrated approach, realist understanding, digital governance, constructivist perspective, US, EU, China, India.*