

ПУБЛИЧНО-ПРАВОВЫЕ (ГОСУДАРСТВЕННО-ПРАВОВЫЕ) НАУКИ

Научная статья

УДК 342.2

DOI: 10.18384/2949-513X-2025-4-14-28

ЦИФРОВОЙ СУВЕРЕНИТЕТ КАК НОВАЯ ПРАВОВАЯ КОНЦЕПЦИЯ

Коданева С. И.

Институт научной информации по общественным наукам РАН, г. Москва, Российская Федерация

e-mail: kodanevas@gmail.com

Поступила в редакцию 18.09.2025

После доработки 12.10.2025

Принята к публикации 25.10.2025

Аннотация

Цель. Анализ подходов к определению цифрового суверенитета и выработка концепции цифрового суверенитета.

Процедура и методы. Ключевым исследовательским методом стал сравнительно-правовой анализ. Проведён контекст-анализ научных публикаций и законодательства различных стран. Применены методы классификации и синтеза для выявления общих и специфических элементов цифрового суверенитета.

Результаты. Доказано, что качественным отличием цифрового суверенитета от традиционного государственного суверенитета являются суверенные права (способность контролировать) над данными. Исходя из этого сделан вывод, что многообразие национальных подходов к концептуализации и правовому регулированию цифрового суверенитета являются не более чем различиями в методах государственного управления, присущих этим странам. На основе этого сформулировано определение цифрового суверенитета.

Теоретическая и/или практическая значимость. Раскрыта сущность цифрового суверенитета как способности управлять данными и сделанном из этого выводе, что существующие в настоящее время противоречия между национальными подходами к пониманию цифрового суверенитета могут быть разрешены путём выработки единых, согласованных подходов к международно-правовому регулированию в данной области.

Ключевые слова: Вестфальская система, государственная юрисдикция, киберпространство, технологическая независимость, управление данными, цифровая автономия

Для цитирования:

Коданева С. И. Цифровой суверенитет как новая правовая концепция // Московский юридический журнал. 2025. № 4. С. 14–28. 2025. <https://doi.org/10.18384/2949-513X-2025-4-14-28>.

Original research article

DIGITAL SOVEREIGNTY AS A NEW LEGAL CONCEPT

S. Kodaneva

*Institute of Scientific Information for Social Sciences (INIION) of the Russian Academy of Sciences,
Moscow, Russian Federation*

e-mail: kodanevas@gmail.com

Received by the editorial office 18.09.2025

Revised by the author 12.10.2025

Accepted for publication 25.10.2025

Abstract

Aim. To analyse approaches to the define digital sovereignty and the development of the digital sovereignty concept.

Methodology. Comparative legal analysis was a key research method In the study. The context analysis of scientific publications and legislation of various countries was carried out. Classification and synthesis methods were applied to identify common and specific elements of digital sovereignty.

Results. It is proved that the qualitative difference between digital sovereignty and traditional state sovereignty is sovereign rights (the ability to control) over data. Based on this, it is concluded that the diversity of national approaches to the conceptualization and legal regulation of digital sovereignty are nothing more than differences in the methods of public administration inherent in these countries. Based on this, the definition of digital sovereignty is formulated.

Research implications. It consists in revealing the essence of digital sovereignty as the ability to manage data and the conclusion drawn from this that the current contradictions between national approaches to understanding digital sovereignty can be resolved by developing unified, coordinated approaches to international legal regulation in this area.

Keywords: Westphalian system, state jurisdiction, cyberspace, technological independence, data management, digital autonomy

For citation:

Kodaneva, S. I. (2025). Digital Sovereignty as a New Legal Concept. In: *Moscow Juridical Journal*, 4, pp. 14–28. <https://doi.org/10.18384/2949-513X-2025-4-14-28>.

Введение

Ещё совсем недавно интернет рассматривался как безграничное глобальное пространство, свободное от государственного вмешательства. Этот взгляд получил широкое распространение благодаря «Декларации независимости киберпространства» Д. П. Барлоу, опубликованной им в 1996 г. При этом такие державы, как США, последовательно отстаивали позицию, согласно которой интернет является общим достоянием, таким же как космос или Мировой океан, а потому в цифровом пространстве невозможен никакой государственный суверенитет. Однако

сегодня очевидно, что подобные взгляды были утопией. Теперь государства стремятся утвердить свою власть в этом пространстве, что порождает доктринальные споры о природе цифрового суверенитета, его соотношении с традиционным суверенитетом, основанным на философских трудах Ж. Бодена, воплотившихся в Вестфальском мире (1648), а также о его содержании и возможности правового закрепления.

В настоящей статье предпринята попытка сравнительного анализа существующих подходов к пониманию цифрового суверенитета и его концептуализации.

Концептуальные подходы к пониманию сущности цифрового суверенитета

Если обратиться к истории, то можно видеть, что вопрос о возможности регулирования интернета прошёл в своём развитии 3 этапа:

1) *ранний этап*, ориентированный на интеграцию рынка и глобальную гармонизацию регулирования с целью создания возможностей для трансграничной торговли и общения (1970–80-е гг.);

2) *период децентрализации и сетевого управления*, когда интернет рассматривался как освобождающая, не имеющая границ сила, подрывающая государственный суверенитет и расширяющая возможности отдельных лиц и гражданского общества (1990-е – 2000-е гг.);

3) *восстановление централизации власти*, формирование платформенного капитализма (2010-е гг. – н. в.).

Концентрация власти на мегаплатформах, рост цифрового авторитаризма и превращение технологических цепочек поставок в геополитическое оружие вновь заставили задуматься о вопросах национального суверенитета. Государство становится центральным действующим лицом, а его суверенитет рассматривается уже не как отмирающий пережиток, но как ответ на современные вызовы.

Анализ концепции цифрового суверенитета следует начинать с определения его соотношения с принципами традиционного суверенитета государства, сформулированными в Вестфальском мирном договоре – территориальной целостности государства и верховенства его власти на своей территории, невмешательства во внутренние дела других государств и суверенного равенства государств. Если переносить эти принципы на киберпространство, то сразу возникают разногласия относительно их применимости, поскольку оно по своей сути нетерриториально, характеризуется транснациональными потоками данных, распределённой инфраструктурой и значительной ролью негосу-

дарственных субъектов, в частности глобальных технологических корпораций [1].

Так, правоведы-конституционалисты полагают, что Вестфальская модель по-прежнему является незыблемой фундаментальной основой суверенитета в цифровой среде. Разница заключается только в категоричности данной позиции. Крайние её сторонники полагают, что государственный суверенитет – это качественный, неделимый и неотъемлемый атрибут государства, проводя тем самым различие между суверенитетом и суверенными правами, которые могут быть ограничены, разделены или переданы по договору. Государство же либо суверенно, либо нет. Следовательно, само по себе понятие цифрового суверенитета является нонсенсом, как и прочие «виды» суверенитета – экономический, идеологический и т. п. [2].

Менее радикальная позиция сводится к тезису о том, что цифровой суверенитет возник как продолжение традиционного вестфальского суверенитета и его интерпретация и реализация в основном определяются геополитической конкуренцией, национальными интересами и различными политическими моделями. Данная позиция основана на том факте, что суверенитет никогда не был статичным, он динамично расширялся на море и в атмосфере. Следовательно, цифровая сфера – это не более чем новое, хотя и самое сложное для определения пространство для расширения государственного суверенитета [3].

В свою очередь политологи обращают внимание на то, что суверенитет имеет двойственную природу. С одной стороны, это состояние бытия – онтологическая характеристика государства, его право на внутреннюю автономию и самостоятельность во внешней политике (суверенитет де-юре). С другой стороны, это способность указанное право реализовать на практике (суверенитет де-факто), которая в настоящее время активно оспаривается, подвергается риску и должна защищаться с помощью конкретной политики, технологий и международного взаимодействия,

поскольку очевидно, что отсутствие второй составляющей делает первую бессмысленной декларацией [4]. Взгляды авторов, опирающихся на данный тезис, заметно отличаются от правоведов-конституционалистов, предлагая широкий спектр подходов к определению цифрового суверенитета, начиная от полного отказа от Вестфальской модели и заканчивая призывами к её переосмыслению.

Так, например, утверждается, что в современном мире существует множество акторов, которые претендуют на суверенитет и, следовательно, можно говорить о множественном суверенитете, включающем помимо государственного цифрового суверенитета наднациональный цифровой суверенитет (например, суверенитет на уровне ЕС), сетевой цифровой суверенитет, цифровой суверенитет коренных народов и общин, корпоративный цифровой суверенитет (платформ), личный цифровой суверенитет (суверенитет человека в киберпространстве, в частности, контроль за использованием своих персональных данных), постколониальный цифровой суверенитет (сопротивление цифровому империализму) [5]. При этом, например, в Германии в дискуссиях присутствует акцент на «цифровом суверенитете на индивидуальном уровне», который заключается в создании с помощью образования «субъектов, обладающих цифровой суверенностью». Таким образом, национальная конкурентоспособность и безопасность напрямую связана с компетенциями граждан, а суверенитет рассматривается как концепция, формируемая снизу вверх, а не навязанная сверху вниз [6].

Некоторые авторы полагают, что цифровой суверенитет как единая концепция вообще не существует, но следует говорить о широком спектре цифровых суверенитетов, развивающихся по-разному в зависимости от положения страны в глобальной иерархии, её колониальной истории и внутренней политики и экономики. Соответственно, цифровой суверенитет – это многомерное явление, включающее помимо юридического и властного контроля

над территорией технический потенциал, экономическую самодостаточность и культурную автономию [7].

Как можно видеть, данный подход основан на признании невозможности для некоторых стран (преимущественно бывших колоний) реализовать цифровой суверенитет де-факто в силу технологической зависимости от стран Запада, которая трактуется как цифровой неокOLONиализм.

Однако большинство авторов всё же обращают внимание на чисто технический аспект – сложность цифровой среды, которая является многослойной и включает в себя физическую инфраструктуру, технические стандарты, программы (алгоритмы), включая платформы, и размещаемый на них или с их помощью контент. Эти слои могут контролироваться различными субъектами, что создаёт проблемы юрисдикции: пакет данных из ЕС, передаваемый по подводному кабелю, принадлежащему американской компании, обрабатывается в индийском дата-центре с помощью платформы, принадлежащей Китаю. Соответственно, формируется сложная топология взаимопроникающих суверенных претензий различных государств и негосударственных субъектов (прежде всего, транснациональных корпораций), которые накладываются друг на друга и переплетаются.

В этой топологии Вестфальская модель, как полагают авторы, неприменима, поскольку суверенитет заключается не в территориальной юрисдикции или стратегической автономии по отношению к другим государствам, а во владении или, по крайней мере, способности контролировать физическую инфраструктуру и методы обработки данных. Иными словами, суверенитет понимается как «право на культурное и политическое самоопределение» в цифровой сфере [8]. Развивая эту мысль, можно сказать, что государство – это уже не просто физическая территория, но политическая концепция, объединившая эту территорию с правовой юрисдикцией над ней и национальной идентичностью. И если для Вестфальской модели ключевым

элементом являются физические границы между государствами, то цифровые границы – это не стены или заборы, а механизмы фильтрации для управления потоком данных, капитала и информации, позволяющие циркулировать в информационном пространстве тому, что рассматривается как юридически дозволенное и блокирующее запрещённый контент или деятельность. При этом цифровые границы включают когнитивную составляющую, когда сами пользователи делят интернет-ресурсы на «свои» и «чужие». Например, китайские пользователи проводят различие между «нейвангом» (внутренней сетью) и «вайвангом» (внешней сетью). Это не просто результат государственной цензуры, но «активная, символическая практика установления границ, осуществляемая самими пользователями, формирующая их поведение, речь и чувство общности» [9]. Иными словами, по мнению сторонников данного подхода, «государственная граница» в эпоху цифровых технологий – это не фиксированная линия, а размытый, многовариантный набор практик.

Государства стремятся выстраивать цифровые границы с помощью законов и инфраструктуры, корпорации влияют на (либо подстраиваются под) государственные границы с помощью условий предоставления услуг и маршрутизации данных, а граждане сами формируют эти границы в своём сознании с помощью повседневных цифровых привычек, страхов и практик.

Сравнительный анализ национальных подходов к цифровому суверенитету

Китай

Подход Китая представляет собой наиболее всеобъемлющую и институционализированную модель государственного контроля над киберпространством в мире. Китайская цифровая инфраструктура изначально создавалась внутри страны и принадлежала ей [10], благодаря «национальному социо-техническому воображению» и политике, основанной на идее государственного суверенитета в кибер-

пространстве как основы политической стабильности и национального возрождения [11]. Правовое отражение этой позиции нашло в белой книге Государственного совета 2010 г. «Интернет в Китае» (согласно которой на территории Китая интернет находится под юрисдикцией суверенитета Китая; сетевой суверенитет Китая должен уважаться и защищаться), а также в ряде законов:

– Закон о кибербезопасности 2016¹ (*The Cybersecurity Law of the People's Republic of China* – 中华人民共和国网络安全法), который закрепил термин «сетевой суверенитет», установив всеобъемлющий государственный контроль над сетевыми операциями и данными);

– Закон о защите данных 2021² (*Data Security Law of the People's Republic of China* – 中华人民共和国数据安全法), который рассматривает данные как «национальное достояние» и устанавливает систему защиты секретных данных;

– Закон о защите личной информации 2021³ (*Personal Information Protection Law of the People's Republic of China* – 中华人民共和国个人信息保护法) – китайский аналог Общего регламента по защите данных ЕС, который предоставляет гражданам страны право на конфиденциальность, однако это право в значительной степени ограничено исключениями, касающимися национальной безопасности и общественных интересов и требованием к операторам данных сотрудничать с органами общественной безопасности и ведомствами госбезопасности).

Техническую основу цифрового суверенитета Китая составляют «Великий брандмауэр» (фильтрация на международных

¹ The Cybersecurity Law of the People's Republic of China [Электронный ресурс]. URL: https://www.cac.gov.cn/2016-11/07/c_1119867116.htm (дата обращения: 10.09.2025).

² Data Security Law of the People's Republic of China [Электронный ресурс]. URL: https://www.cac.gov.cn/2021-06/11/c_1624994566919140.htm (дата обращения: 09.09.2025).

³ Personal Information Protection Law of the People's Republic of China [Электронный ресурс]. URL: https://www.cac.gov.cn/2021-08/20/c_1631050028355286.htm (дата обращения: 09.09.2025).

шлюзах для блокирования доступа к иностранным веб-сайтам и сервисам); обязательная проверка личности для доступа в интернет и получения услуг; система социального кредитования, включающая интеграцию онлайн- и офлайн-поведения в комплексную систему социального управления, и национальная цифровая экосистема, основанная на создании местных альтернатив глобальным платформам.

Цели политической стабильности в Китае тесно переплетены с другими целями, включая национальную безопасность, технологические инновации, экономический рост и социальное развитие. Таким образом, акцент на сетевой безопасности и развитии инфраструктуры, свойственный более ранней политике Китая, затем сместился в сторону регулирования контента, а в последнее время – цифровой экономики [12]. При этом законодательство Китая, как и право ЕС, всё больше приобретает экстерриториальные характеристики, т. е. Китай стремится распространить свои правовые стандарты зарубежом посредством инициативы «Цифровой шёлковый путь», двух- и многосторонних соглашений, одновременно принимая меры для противостояния иностранным правилам, особенно в отношении данных, которые страна считает дискриминационными [13].

Россия

Российский подход к цифровому суверенитету довольно близок с китайским. Он основан на трактовке целостности государственного суверенитета как права контроля над территорией. Хотя следует признать, что на первоначальном этапе в 1990-е гг. Россия придерживалась модели свободного интернета, практически не регулируя и не контролируя данную сферу. Изменения произошли, как и в ЕС, после разоблачений Э. Сноудена, серии «цветных революций» и «Арабской весны».

Цифровой суверенитет в российской трактовке – это, прежде всего, защита традиционного государственного суверенитета в информационном пространстве от

цифровой гегемонии западных компаний и ценностей. Иными словами, в России цифровой суверенитет связан с обеспечением национальной информационной безопасности, которая понимается широко и включает в себя как традиционную кибербезопасность (т. е. защищённость критически важной инфраструктуры и персональных данных), так и собственно информационную безопасность (недопущение распространения незаконного контента).

Его концептуальную основу составляют Доктрина информационной безопасности РФ, утверждённая Указом Президента РФ от 05.12.2016 № 646, которая определяет 4 основные сферы национальных интересов (личность, общество, государство, стратегическое сдерживание), Стратегия национальной безопасности РФ, утверждённая Указом Президента РФ от 02.07.2021 № 400, согласно которой информационная безопасность является одним из ключевых компонентов национальной безопасности, внешние информационные кампании представлены как угроза конституционному строю России и обозначена необходимость защиты населения от деструктивных информационно-психологических воздействий.

Правовую основу обеспечения цифрового суверенитета РФ составляют:

– Федеральный закон № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»¹ – содержит требования о нахождении на территории РФ баз персональных данных граждан РФ;

– Федеральный закон № 374-ФЗ «О внесении изменений в Федеральный закон “О противодействии терроризму” и отдельные законодательные акты Российской Федерации

¹ Федеральный закон от 21.07.2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях» // СПС Консультант Плюс.

Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности»¹ – обязывает операторов связи хранить на территории РФ информацию о коммуникациях и предоставлять к ней доступ правоохранным органам;

– Федеральный закон № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации»»² – направлен на защиту национального сегмента интернета от внешних угроз, предусматривает создание национальной системы маршрутизации интернет-трафика, инфраструктуры, которая позволит обеспечить работоспособность российских интернет-ресурсов в случае невозможности подключения к зарубежным корневым серверам, минимизацию передачи за рубеж данных, которыми обмениваются между собой российские пользователи, создание национальной системы доменных имён;

– Федеральный закон № 187-ФЗ «О безопасности критически важной информационной инфраструктуры»³ – создаёт систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ;

– Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации»⁴ – регулирует статус информации в РФ, права на её получение

и распространение, а также запрет на распространение незаконного контента и правила его удаления;

– Федеральный закон № 152-ФЗ «О персональных данных»⁵ – содержит правила защиты персональных данных, в целом аналогичные тем, что установлены в Общем регламенте по защите данных ЕС;

– Федеральный закон № 289-ФЗ «Об отдельных вопросах регулирования платформенной экономики в Российской Федерации»⁶ – содержит требования к торговым платформам, направленные на защиту прав пользователей, безопасности цифровой среды и обеспечение единства экономического пространства РФ.

Помимо этого, в стране действует значительный объём подзаконных актов, которые в совокупности образуют один из самых всеобъемлющих и комплексных подходов к регулированию цифрового суверенитета в мире. Однако на практике реализация данной модели цифрового суверенитета сталкивается с рядом сложностей, вызванных технологической зависимостью от иностранных производителей оборудования и платформ (которая в настоящее время постепенно преодолевается), широким использованием VPN и других средств обхода, ограничениями пропускной способности для эффективной фильтрации трафика. Россия пытается решить по крайней мере часть этих проблем за счёт развития отечественных ИТ-гигантов и платформ (Яндекс, ВКонтакте, Mail.ru, Rutube, Ozon, Wildberries и др.), а также взаимодействия с частным сектором.

Таким образом, российская модель цифрового суверенитета представляет собой альтернативное видение в глобальных дебатах по цифровому управлению, в рамках которого государственный контроль, безопасность и цивилизационные особенности ставятся во главу угла.

¹ Федеральный закон от 06.07.2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон “О противодействии терроризму” и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» // СПС Консультант Плюс.

² Федеральный закон от 01.05.2019 г. № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации»» // СПС Консультант Плюс.

³ Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критически важной информационной инфраструктуры» // СПС Консультант Плюс.

⁴ Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СПС Консультант Плюс.

⁵ Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СПС Консультант Плюс.

⁶ Федеральный закон от 31.07.2025 № 289-ФЗ «Об отдельных вопросах регулирования платформенной экономики в Российской Федерации» // СПС Консультант Плюс.

Европейский Союз (ЕС)

Подход ЕС к цифровому суверенитету значительно изменился со времён концепции «глобального информационного общества» 1990-х гг. Поворотный момент наступил после разоблачений Э. Сноудена в 2013 г., которые выявили уязвимости и зависимость Европы. В результате стремление ЕС к цифровому суверенитету является частью более широкой стратегии безопасности и управления, поскольку Союз стремится создавать независимые инфраструктуры и снижать зависимость от иностранных технологий [14].

Интересно, что несмотря на то, что концепция стала центральной в политических дебатах по управлению данными, регулированию платформ и кибербезопасности, целостное видение цифрового суверенитета в ЕС отсутствует [15]. Речь скорее идёт о стратегической автономии посредством регулирования и использования «Брюссельского эффекта» (способность в одностороннем порядке регулировать глобальные рынки, устанавливая стандарты, которые де-факто становятся глобальными требованиями) [16]. Достигается это как за счёт экономического веса ЕС в мире, так и за счёт развитого правового регулирования различных областей цифровой сферы, включающего Общий регламент по защите данных (*General Data Protection Regulation 2016/679, GDPR, 2016*), устанавливающий строгие стандарты защиты данных и имеющий выраженный экстерриториальный характер; Закон о цифровых услугах (*Digital Services Act, 2020*) и Закон о цифровых рынках (*Digital Markets Act, 2020*), направленные на то, чтобы сделать онлайн-среду безопасной и заслуживающей доверия, они регулируют подотчётность платформ и обеспечивают честную конкуренцию, пресекая антиконкурентную практику «платформ-привратников»; Закон об управлении данными (*Data Governance Act, 2022*), упрощающий обмен данными при сохранении контроля над ними.

Отличительной чертой подхода ЕС является его идеологическая опора на «евро-

пейские ценности», хотя точного и разделяемого даже в самой Европе определения, что именно они подразумевают, на сегодняшний день не существует.

США

Как известно, Соединённые Штаты Америки долгое время позиционировали себя (и риторически продолжают это делать) как защитника «свободы интернета», отрицая цифровой суверенитет государства как угрозу свободе слова. Фактически в основе данного подхода лежало стремление защитить интересы американских цифровых транснациональных корпораций.

Однако со временем данный подход стал меняться. Во-первых, цифровые технологии стали использоваться правительством США в качестве инструмента принуждения. Например, SWIFT во время иранского кризиса 2012 г. был использован в качестве оружия [17]. Во-вторых, фактически на своей территории США контролируют деятельность цифровых корпораций. Это пример технационализма и функционального цифрового суверенитета¹ (или корпоративного цифрового суверенитета), реализуемого посредством не территориальных, но юрисдикционных притязаний, основанных на тесном сотрудничестве с частными транснациональными корпорациями, которым даже передаётся часть государственных функций, таких как управление контентом, контроль инфраструктуры, установление стандартов и сбор данных по запросам органов разведки.

Правовую основу для данной модели цифрового суверенитета составляет, прежде всего, Закон США об облачных технологиях (*Clarifying Lawful Overseas Use*

¹ Функциональный цифровой суверенитет – это модель государственной власти в цифровой сфере, при которой суверенитет понимается не как абсолютный, неделимый или формально-юридический атрибут государственности (классическая вестфальская модель), а как способность государства к самостоятельному и независимому принятию решений, осуществлению нормативного контроля и воздействия на определённые элементы цифровой экосистемы вне связи с территориальной юрисдикцией.

of Data Act (CLOUD Act), 2018)¹, который закрепил право органов власти США получать доступ к данным, находящимся на серверах, размещённых в других государствах, если эти сервера принадлежат американским компаниям. Помимо этого, правительство США стремится не допустить усиления своего основного конкурента – Китая – и ограничить его влияние на американское общество посредством использования цифровых информационных технологий.

Правовыми средствами решения этих задач являются Закон о защите американцев от приложений, контролируемых иностранными противниками (*Protecting Americans from Foreign Adversary Controlled Applications Act (PAFACA)*, 2024²), согласно которому социальная сеть TikTok или должна быть продана американской компании, или будет заблокирована; запрет строительства Huawei сетей 5G, ограничение поставок полупроводниковых технологий в Китай посредством таможенного регулирования и т. д.

Индия

Подход Индии к цифровому суверенитету отражает её статус «Державы Юга» – крупной развивающейся экономики со значительными технологическими амбициями, которая реализует собственную версию «государственного предпринимательства», основанного на индийском национализме при цифровом государственном строительстве [18]. Изначально правительство реализовало Национальный план электронного управления, принятый в 2006 г., а начиная с 2015 г. премьер-министр Н. Моди запустил программу «Цифровая Индия», направленную на превращение Индии в

«общество с «цифровыми возможностями и экономикой знаний». Особенностью Индии является «Индийский стек» (*India Stack*), который состоит из нескольких крупномасштабных проектов в области цифровой общественной инфраструктуры для цифровой идентификации (*Aadhaar*), электронных платежей (*UPI*) и обмена данными. При этом *Aadhaar* является крупнейшей в мире биометрической базой данных (1,3 млрд жителей), позволяющей получать государственные услуги онлайн. Это особая модель цифрового суверенитета, основанная не на регулировании или контроле, а на государственной инфраструктуре [7].

Правовой основой реализацией данного подхода являются:

– Закон о защите цифровых персональных данных (*The Digital Personal Data Protection Act, 2023*)³, который устанавливает стандарты защиты данных при сохранении возможности доступа к ним для государственных органов;

– Закон Индии об информационных технологиях (*Information Technology Act, 2000*)⁴, который закрепил ответственность посредников и правила регулирования контента;

– Закон Индии о телекоммуникациях (*The Telecommunication Act, 2023*)⁵ – новый всеобъемлющий акт, заменяющий акты колониальной эпохи, предоставляющий правительству полномочия в области национальной безопасности (перехват, отключения), а также направленный на стимулирование отечественного производства и сокращение зависимости от зарубежных компаний.

¹ Clarifying Lawful Overseas Use of Data Act [Электронный ресурс]. URL: <https://www.govinfo.gov/content/pkg/COMPS-15475/pdf/COMPS-15475.pdf#page=624> (дата обращения: 09.09.2025).

² Protecting Americans from Foreign Adversary Controlled Applications Act [Электронный ресурс]. URL: <https://www.congress.gov/bill/118th-congress/house-bill/7521> (дата обращения: 09.09.2025).

³ The Digital Personal Data Protection Act [Электронный ресурс]. URL: <https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf> (дата обращения: 10.09.2025).

⁴ Information Technology Act [Электронный ресурс]. URL: https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf (дата обращения: 10.09.2025).

⁵ The Telecommunication Act [Электронный ресурс]. URL: <https://egazette.gov.in/WriteReadData/2023/250880.pdf> (дата обращения: 10.09.2025).

При этом Индия ориентирована на сотрудничество с западными компаниями. В частности, в этой стране запрещены китайские приложения (*TikTok*, *WeChat*), правительство Индии участвует в альянсе «*Quad*», созданным в 2007 г. США совместно с Японией и Новой Зеландией в противовес Китаю [19].

ЮАР

Южная Африка представляет собой «колеблющееся государство» в цифровой геополитике – региональную державу с ограниченными ресурсами, балансирующую между крупными цифровыми державами. Страна сталкивается с «двойными цифровыми парадоксами»: поиск выгод от цифрового развития при одновременном устранении угроз кибербезопасности и обеспечении баланса между обеспечением безопасности и защитой прав.

Подход страны определяется стремлением к лидерству в регионе, с одной стороны, и опасениями нового «цифрового колониализма» со стороны как западных, так и китайских технологических компаний, с другой стороны. Государство владеет миноритарными пакетами акций в компаниях телекоммуникационной инфраструктуры, принадлежащих иностранным фирмам, и придерживается децентрализованного подхода, позволяя национальным и иностранным технологическим компаниям свободно конкурировать.

Правовую основу цифрового суверенитета ЮАР составляют:

– Закон о защите личной информации (*South Africa's Protection of Personal Information Act, 2013*)¹, разработанный по аналогии с Общим регламентом по защите данных ЕС;

– Закон о киберпреступности (*The Cybercrimes Act, 2021*)²;

– Национальная политика в области данных и облака (*National Policy on Data and Cloud, 2024*)³, направленная на регулирование вопросов управления цифровым облаком и обеспечение локализации данных.

Данная модель представляет собой попытку добиться цифрового суверенитета, несмотря на высокую технологическую зависимость. При этом ЮАР стремится позиционировать себя как регионального лидера, в частности, оказывая влияние на правовую базу других стран Африки, выступая посредником между западными, китайскими и африканскими цифровыми интересами, а на международном уровне призывая к более справедливому глобальному цифровому управлению. Таким образом, ЮАР представляет собой яркий пример того, как развивающиеся страны пытаются добиться цифрового суверенитета.

Кратко представим различные модели цифрового суверенитета (табл. 1).

Заключение

Проведённый анализ подходов различных государств к пониманию содержания цифрового суверенитета позволяет выделить основные элементы, которые принято к нему относить: это контроль над инфраструктурой, технологиями, распространяемым в сети контентом и данными, а также экономической активностью.

Однако такая широкая трактовка цифрового суверенитета представляется принципиально неверной. Если исходить из того, что государственный суверенитет составляет определённый набор элементов (территориальный суверенитет, юрисдикционный суверенитет, информационный суверенитет⁴, технологический

¹ South Africa's Protection of Personal Information Act [Электронный ресурс]. URL: https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf (дата обращения: 10.09.2025).

² The Cybercrimes Act [Электронный ресурс]. URL: [https://www.gov.za/documents/acts/cybercrimes-](https://www.gov.za/documents/acts/cybercrimes-act-19-2020-english-afrikaans-01-jun-2021)

[act-19-2020-english-afrikaans-01-jun-2021](https://www.gov.za/documents/acts/cybercrimes-act-19-2020-english-afrikaans-01-jun-2021) (дата обращения: 10.09.2025).

³ National Policy on Data and Cloud. URL: https://www.gov.za/sites/default/files/gcis_document/202406/50741gen2533.pdf

⁴ Информационный суверенитет – это юридическое свойство (признак) государства как особого субъекта информационно-правовых отношений,

Таблица 1 / Table 1

Модели цифрового суверенитета / Digital sovereignty models

Модель	Страны	Концепция цифрового суверенитета	Механизмы реализации
Цифровой суверенитет	Китай, Россия	Цифровой суверенитет как абсолютная государственная власть над ограниченным киберпространством	Техническая фильтрация контента на границах, правовые механизмы контроля за киберпространством, отечественные технологии и платформы
Регулятивный суверенитет	ЕС	Цифровой суверенитет как способность осуществлять глобальное управление посредством правового регулирования	Экстерриториальное регулирование, установление глобальных стандартов, продвижение своих ценностей как основы для глобального регулирования
Корпоративный суверенитет/функциональный суверенитет	США	Глобальный суверенитет через власть ТНК и юрисдикционные притязания	Законодательное закрепление экстерриториальности цифрового суверенитета США, управление цифрового средой через частные корпорации
Технологический суверенитет	Индия	Суверенитет через управляемые государством цифровые общественные блага	Национальная цифровая инфраструктура: облачные сервисы, система идентификации, платёжная система, управление данными
Прагматическая зависимость	ЮАР	Ограниченный суверенитет в условиях цифровой зависимости	Децентрализация управления, конкуренция иностранных компаний на национальном рынке, позиционирование себя как регионального лидера в продвижении правового регулирования

Источник: составлено автором

суверенитет¹, экономический суверенитет² и цифровой суверенитет), то очевидно, что каждый из этих элементов является самодостаточным. То есть одно и то же свой-

осуществляющего их правовое регулирование как в пределах своей территории (внутригосударственное информационное пространство), экстерриториальных режимов, так и при участии в международно-правовом регулировании (глобальное и региональное информационное пространство) [20]

¹ Технологический суверенитет – это способность страны самостоятельно создавать, контролировать и применять критически важные технологии, обеспечивая экономическую и национальную безопасность [21].

² Экономический суверенитет – это свойство государства, при котором оно способно самостоятельно принимать решения в сфере экономики и проводить экономическую политику [20].

ство государства не может одновременно входить в 2 и более элемента его суверенитета (например, территориальный суверенитет – это физический контроль над территориями и всем, что находится на ней, над ней или под ней, в то время как юрисдикционный суверенитет – это верховенство национального права на данной территории). Включение же в цифровой суверенитет всего, что было перечислено выше, неизбежно приведёт к пересечению между цифровым и прочими элементами суверенитета, чего, в принципе, быть не может.

Так, контроль над инфраструктурой (дата-центры, кабели и т. п.) явно отно-

сится к территориальному суверенитету, коль скоро они физически находятся на территории государства. Если же они принадлежат по праву собственности частному юридическому лицу, но физически располагаются на территории иного государства, то, как и в отношении иных объектов собственности, суверенитет государства на них не может распространяться.

Юрисдикционный суверенитет государства традиционно может действовать только на его территории, поэтому попытки распространить его на территорию других государств недопустимы. Речь может идти только о выборе сторонами гражданско-правовых отношений применимого права, т. е. юрисдикции разрешения спора.

Контроль над технологиями, используемым в цифровом пространстве очевидно составляет часть технологического суверенитета, который означает наличие в стране критических и сквозных технологий, обеспечивающих устойчивую возможность государства и общества достигать собственные национальные цели развития и реализовывать национальные интересы¹.

Способность государства формировать ценности, нормы и принципы, принятые в киберпространстве, а также контролировать и управлять распространяемым в стране контентом является признаком информационного суверенитета.

Наконец, способность контролировать деятельность цифровых платформ, пресекая злоупотребления с их стороны как в вопросах конкуренции, так и в сфере распространяемого с их помощью контента, а также регулировать владение и распоряжение цифровыми активами – это основа экономической безопасности государства, т. е. его экономического суверенитета.

Исходя из того, что цифровой суверенитет не может подменять собой ни один из перечисленных выше элементов государственного суверенитета, то все указанные явления, по сути, являются ни чем иным,

как традиционными общественными отношениями, только осуществляемыми в цифровой среде, что не отменяет для них общих правил определения пределов национального суверенитета. Фактически единственным объектом, выходящим за эти рамки и специфическим для цифровой среды, является суверенитет данных. Он включает правовое регулирование вопросов сбора, хранения, обработки и передачи данных, в т. ч. правила их локализации (предписывающие, чтобы определённые данные оставались в пределах национальных границ).

Приведённые выше сравнение национальных подходов к цифровому суверенитету показывает признание той роли, которую данные играют в современном мире и, соответственно, желания государств их контролировать (например, для Китая данные – это «национальное достояние»). Иными словами, цифровой суверенитет заключается именно в способности государства реализовать своё суверенное право (осуществлять контроль) в отношении данных.

Подтверждением этому служит то, что, согласно Указу Президента РФ № 203, цифровая экономика – это хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде. Иными словами, основой цифровой трансформации стали технологии обработки больших массивов данных, а владение самими данными и способность их обрабатывать являются квалифицирующими признаками цифровизации и всех связанных с ней явлений (будь то цифровая экономика или цифровой суверенитет).

При этом суверенитет (контроль) над данными заключается в способности государства осуществлять их правовое регулирование в форме нормативно установленных ограничений по способам и пределам их использования для различных целей, требований их локализации (т. е. хранении на территории государства) и ограничению их передачи за пределы государства (это могут быть правила о том, какие данные можно передавать свободно, какие с согласия их субъ-

¹ Распоряжение Правительства РФ от 20.05.2023 г. № 1315-р «Об утверждении Концепции технологического развития на период до 2030 г.» // СПС Консультант Плюс.

екта, а какие – только с согласия уполномоченных органов власти и/или процедурные правила, например, как в Китае).

Что же касается рассмотренных выше различий в подходах разных государств к пониманию цифрового суверенитета, то это скорее разница в методах и инструментах реализации этого суверенного права. Однако если говорить объективно, то способы осуществления суверенных прав в отношении рассмотренных элементов суверенитета всегда различаются в зависимости от политических систем, технологического и экономического развития, стратегических приоритетов, а также исторических корней и мировоззренческих позиций страны. Поэтому данные различия в подходах к цифровому суверенитету не должны вводить в заблуждение.

Модели «корпоративного суверенитета» (США), «цифрового суверенитета» (Китай/Россия) и «регулятивного суверенитета» (ЕС) представляют собой конкурирующие нормативные подходы к регулированию вопросов сбора, хранения, использования и передачи данных. Следовательно, за-

дачей сначала научного, а затем и международного политического сообщества является выработка единых, согласованных подходов к правовому регулированию в данной области.

В этом контексте Россия вполне может претендовать на одну из ведущих ролей в мире, поскольку обладает наиболее комплексной и проработанной правовой базой, а следовательно, может предлагать готовые правовые подходы к регулированию вопросов цифрового суверенитета на международном уровне.

В качестве же концептуальной основы для начала такой дискуссии о формулировании единого подхода к пониманию цифрового суверенитета, представляется возможным, опираясь на определение государственного суверенитета, сформулированное А. Б. Венгеровым¹, предложить следующее определение: *цифровой суверенитет – это обладание правом и возможностью осуществлять политику управления данными от имени всего общества внутри страны.*

ЛИТЕРАТУРА

1. Ruohonen J. The treachery of images in the digital sovereignty debate // *Minds and Machines*. 2021. Vol. 31. № 3. P. 439–456. DOI: 10.1007/s11023-021-09566-7.
2. Терентьева Л. В. Концепция суверенитета государства в условиях глобализационных и информационно-коммуникационных процессов // *Право. Журнал Высшей школы экономики*. 2017. № 1. С. 187–200.
3. Zinovieva E. Evolution of the Concept “Territorial Sovereignty” in the Digital Age // *Proceedings of Topical Issues in International Political Geography*. 2022. P. 187–195. DOI: 10.1007/978-3-031-50407-5_15.
4. Сюй Хао, Сюй Чан Киберпространство и суверенитет: как сетевое взаимодействие формирует национальную автономию // *Социально-гуманитарные знания*. 2025. № 6. С. 251–256.
5. Jiang M., Belli L. Contesting Digital Sovereignty: Untangling a Complex and Multifaceted Concept // *Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance* / eds. M. Jiang, L. Belli. Cambridge: Cambridge University Press, 2024. P. 1–24.
6. Glasze G., Cattaruzza A., Douzet F., et al. Contested Spatialities of Digital Sovereignty // *Geopolitics*. 2023. Vol. 28. № 2. P. 919–958. DOI: 10.1080/14650045.2022.2050070
7. Min Jiang. Models of State Digital Sovereignty From the Global South: Diverging Experiences From China, India and South Africa // *Policy and Internet*. 2024. Vol. 16. P. 727–738. DOI: 10.1002/poi3.427
8. Pierucci F. Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace // *Digital Society*. 2025. Vol. 4. P. 27. DOI: 10.1007/s44206-025-00189-4.
9. Zhang Ch., Morris C. Borders, bordering and sovereignty in digital space // *Territory, Politics,*

¹ Согласно А. Б. Венгерову, государственный суверенитет – это верховенство и независимость от какой-либо иной власти, обладание правом и возможностью осуществлять внутреннюю и внешнюю политику от имени всего общества внутри и вне страны [22]

- Governance. 2023. Vol. 11. № 6. P. 1051–1058. DOI: 10.1080/21622671.2023.2216737.
10. Mihelj S. Platform nations // *Nations and Nationalism*. 2023. Vol. 29. № 1. P. 10–24. DOI: 10.1111/nana.12912.
 11. Morris C. Digital displacement: The spatialities of contentious politics in China's digital territory // *Transactions of the Institute of British Geographers*. 2022. Vol. 47. № 4. P. 1075–1089. DOI: 10.1111/tran.12559.
 12. Miao W., Jiang M., Pang Y. Historicizing Internet Regulation in China: A Meta-Analysis of Chinese Internet Policies (1994–2017) // *International Journal of Communication*. 2021. Vol. 15. P. 2003–2026. DOI: 10.2139/ssrn.4852245.
 13. Cong W. The Spatial Expansion of China's Digital Sovereignty: Extraterritoriality and Geopolitics // *Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance* / eds. M. Jiang, L. Belli. Cambridge: Cambridge University Press, 2024. P. 63–80.
 14. Bellanova R., Carrapico H., Duez D. Digital sovereignty and European security integration: An introduction // *European Security*. 2022. Vol. 31. № 3. P. 337–355. DOI: 10.1080/09662839.2022.2101887.
 15. Roberts H., Cowls J., Casolari F., et al. Safeguarding European values with digital sovereignty: An analysis of statements and policies // *Internet Policy Review*. 2021. Vol. 10. № 3. P. 1–26.
 16. Bradford A. *The Brussels effect: How the European Union rules the world*. Oxford: Oxford University Press, 2020. 404 p.
 17. Farrell H., Newman A. L. Weaponized interdependence: How global economic networks shape state coercion // *International Security*. 2019. Vol. 44. № 1. P. 42–79.
 18. Kumar A., Thussu D. Media, Digital Sovereignty and Geopolitics: The Case of the Tiktok Ban in India // *Media, Culture and Society*. 2023. Vol. 45. № 8. P. 1583–1599.
 19. Athique A., Ilavarasan V., Parthasarathi V., et al. *Communications, Media and Internet Concentration in India 2019–2021*. Global Media and Internet Concentration Project, 2024. 98 p.
 20. Варлен М. В. Информационный, технологический, экономический и финансовый суверенитет как новейшие типы автономности // *Вестник Университета имени О. Е. Кутафина (МГЮА)*. 2023. № 9. С. 214–222.
 21. Пуляев А. В. Концепция технологического суверенитета как система правоотношений // *Законодательство*. 2024. № 10. С. 56–65.
 22. Венгеров А. Б. *Теория государства и права*. М., 2005. 608 с.

REFERENCES

1. Ruohonen, J. (2021). The Treachery of Images in the Digital Sovereignty Debate. In: *Minds and Machines*, 31-3, 439–456. DOI: 10.1007/s11023-021-09566-7.
2. Terentyeva, L. V. (2017). The Concept of State Sovereignty in the Context of Globalization and Information and Communication Processes. In: *Law. Journal of the Higher School of Economics*, 1, 187–200 (in Russ.).
3. Zinovieva, E. (2022). Evolution of the Concept “Territorial Sovereignty” in the Digital Age. In: *Proceedings of Topical Issues in International Political Geography*. 2022. Springer, pp. 187–195. DOI: 10.1007/978-3-031-50407-5_15.
4. Xu Hao, Xu Chan. (2025). Cyberspace and Sovereignty: How Networking Shapes National Autonomy. In: *Social and Humanitarian Knowledge*, 6, 251–256 (in Russ.).
5. Jiang M., Belli L. (2024). Contesting Digital Sovereignty: Untangling a Complex and Multifaceted Concept. In: *Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance*. Cambridge: Cambridge University Press, pp. 1–24.
6. Glasze, G., Cattaruzza, A., Douzet, F., et al. (2023). Contested Spatialities of Digital Sovereignty. In: *Geopolitics*, 28-2, 919–958. DOI: 10.1080/14650045.2022.2050070.
7. Min Jiang. (2024). Models of State Digital Sovereignty from the Global South: Diverging Experiences from China, India and South Africa. In: *Policy and Internet*, 16, 727–738. DOI: 10.1002/poi3.427.
8. Pierucci, F. (2025). Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace. In: *Digital Society*, 4, 27. DOI: 10.1007/s44206-025-00189-4.
9. Zhang, Ch. & Morris, C. (2023). Borders, Bordering and Sovereignty in Digital Space. In: *Territory, Politics, Governance*, 11-6, 1051–1058. DOI: 10.1080/21622671.2023.2216737.
10. Mihelj, S. (2023). Platform Nations. In: *Nations and Nationalism*, 29-1, 10–24. DOI: 10.1111/nana.12912.

11. Morris C. (2022). Digital Displacement: The Spatialities of Contentious Politics in China's Digital Territory. In: *Transactions of the Institute of British Geographers*, 47-4, 1075–1089. DOI: 10.1111/tran.12559.
12. Miao, W., Jiang, M. & Pang, Y. (2021). Historicizing Internet Regulation in China: A Meta-Analysis of Chinese Internet Policies (1994–2017). In: *International Journal of Communication*, 15, 2003–2026. DOI: 10.2139/ssrn.4852245.
13. Cong, W. (2024). The Spatial Expansion of China's Digital Sovereignty: Extraterritoriality and Geopolitics. In: *Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance*. Cambridge: Cambridge University Press, 63–80.
14. Bellanova, R., Carrapico, H. & Duez, D. (2022). Digital Sovereignty and European Security Integration: An Introduction. In: *European Security*, 31, 3, 337–355. DOI: 10.1080/09662839.2022.2101887.
15. Roberts, H., Cows, J., Casolari, F., et al. (2021). Safeguarding European values with digital sovereignty: An analysis of statements and policies. In: *Internet Policy Review*, 10-3, 1–26.
16. Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford: Oxford University Press.
17. Farrell, H. & Newman, A. L. (2019). Weaponized Interdependence: How Global Economic Networks Shape State Coercion. In: *International Security*, 44-1, 42–79.
18. Kumar, A. & Thussu, D. (2023). Media, Digital Sovereignty and Geopolitics: The Case of the Tiktok Ban in India. In: *Media, Culture and Society*, 45-8, 1583–1599.
19. Athique, A., Ilavarasan, V., Parthasarathi, V., et al. (2024). *Communications, Media and Internet Concentration in India 2019–2021*. Global Media and Internet Concentration Project.
20. Varlen, M. V. (2023). Information, Technological, Economic and Financial Sovereignty as the Latest Types of Autonomy. In: *Courier of Kutafin Moscow State Law University (MSAL)*, 9, 214–222 (in Russ.).
21. Pulyaev, A. V. (2024). The Concept of Technological Sovereignty as a System of Legal Relations. In: *Legislation*, 10, 56–65 (in Russ.).
22. Vengerov, A. B. (2005). *Theory of State and Law*. Moscow (in Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Коданева Светлана Игоревна (г. Москва) – кандидат юридических наук, доцент, старший научный сотрудник Отдела правоповедения Института научной информации по общественным наукам РАН; ORCID: 0000-0002-8232-9533; e-mail: kodanevas@gmail.com

INFORMATION ABOUT THE AUTHOR

Svetlana I. Kodaneva (Moscow) – Cand. Sci. (Law), Assoc. Prof., Senior Researcher, Department of Law, Institute of Scientific Information for Social Sciences (INION) of the Russian Academy of Sciences; ORCID: 0000-0002-8232-9533; e-mail: kodanevas@gmail.com