

Дата поступления рукописи в редакцию: 11.06.2026 г.

DOI: 10.24412/2076-1503-2026-7-796-800

Дата принятия рукописи в печать: 03.08.2026 г.

ОРЕШНИКОВА Ксения Сергеевна,

Преподаватель кафедры публичного права Государственного университета аэрокосмического приборостроения,

e-mail: shkunova.ksenia@mail.ru

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЦИФРОВОГО СУВЕРЕНИТЕТА

Аннотация. В статье исследуются теоретические и правовые аспекты цифрового суверенитета как категории, отражающей способность государства самостоятельно определять правила функционирования цифровой среды, обеспечивать устойчивость национальной инфраструктуры связи и контроля над критически значимыми информационными процессами.

Особое внимание уделяется соотношению цифрового суверенитета с конституционным принципом государственного суверенитета, правом на неприкосновенность частной жизни, режимом персональных данных и правовым регулированием критической информационной инфраструктуры. Показано, что цифровой суверенитет не сводится к изоляции национального сегмента сети Интернет, а предполагает юридически выверенный баланс между технологической независимостью, доступностью цифровых сервисов и гарантиями прав и свобод человека.

На основе анализа Конституции Российской Федерации, федеральных законов об информации, связи, персональных данных и безопасности критической информационной инфраструктуры, а также научных публикаций выявляются ключевые проблемы нормативного регулирования: фрагментарность понятийного аппарата, зависимость от зарубежных технологических решений, риски избыточного ограничения доступа к информации и недостаточная определенность механизмов ответственности операторов цифровых платформ. Сделан вывод о необходимости дальнейшего развития законодательства и выработки целостной модели правового обеспечения цифрового суверенитета Российской Федерации.

Ключевые слова: цифровой суверенитет, информационное право, критическая информационная инфраструктура, персональные данные, технологическая независимость, цифровая безопасность, государственное регулирование.

ORESHNIKOVA Ksenia Sergeevna,

Lecturer, Department of Public Law State University of Aerospace Instrumentation

LEGAL REGULATION OF DIGITAL SOVEREIGNTY

Annotation. The article examines the theoretical and legal aspects of digital sovereignty as a category reflecting a state's ability to independently determine the rules governing the digital environment, ensure the resilience of national communications infrastructure, and control critically important information processes.

Special attention is given to the relationship between digital sovereignty and the constitutional principle of state sovereignty, the right to privacy, the legal regime of personal data, and the regulation of critical information infrastructure. The study shows that digital sovereignty cannot be reduced to the isolation of the national segment of the Internet; rather, it presupposes a legally balanced combination of technological independence, accessibility of digital services, and guarantees of human rights and freedoms.

Based on an analysis of the Constitution of the Russian Federation, federal laws on information, communications, personal data, and critical information infrastructure security, as well as doctrinal

ОБРАЗОВАНИЕ И ПРАВО № 7 • 2026

publications, the article identifies the main regulatory problems: fragmentation of the conceptual framework, dependence on foreign technological solutions, risks of excessive restriction of access to information, and insufficiently defined liability mechanisms for digital platform operators. The author concludes that further development of legislation and a coherent model for the legal support of digital sovereignty in the Russian Federation are required.

Key words: *digital sovereignty, information law, critical information infrastructure, personal data, technological independence, digital security, state regulation.*

Цифровизация государственного управления, бизнеса и повседневных коммуникаций изменила не только способы обмена информацией, но и саму архитектуру публичной власти, поскольку в цифровой среде государство вынуждено обеспечивать одновременно открытость сервисов, устойчивость инфраструктуры и защиту национальных интересов. В результате вопрос о цифровом суверенитете перестал быть сугубо технологическим и приобрел отчетливо правовой характер, требующий осмысления через призму конституционного строя, информационной безопасности и гарантий прав человека [1,2].

В доктрине цифровой суверенитет понимается по-разному: как способность государства самостоятельно определять правила цифровой среды, как совокупность мер по защите инфраструктуры и данных либо как более широкий правовой режим, обеспечивающий независимость критических цифровых процессов от внешнего контроля и внешних центров принятия решений [8-11]. При этом наиболее продуктивным представляется подход, согласно которому цифровой суверенитет не тождествен закрытию национального сегмента сети Интернет, а выражает право и обязанность государства устанавливать правила функционирования цифрового пространства, не разрушая при этом свободу информации и международное взаимодействие.

Актуальность темы усиливается тем, что зависимость от иностранных программных платформ, сетевого оборудования, облачных сервисов и трансграничных каналов передачи данных создает для государства не только технологические, но и юридические риски. К таким рискам относятся невозможность полного контроля над маршрутами трафика, утрата управляемости критической информационной инфраструктурой, а также вероятность неправомерного вмешательства в процессы хранения и использования данных граждан и организаций [5-7].

Методологическую основу исследования составили формально-юридический, системный, сравнительно-правовой и доктринальный методы. Их применение позволило рассмотреть цифровой

суверенитет не как абстрактную политическую категорию, а как совокупность нормативных предписаний, организационных процедур и гарантий, направленных на обеспечение самостоятельности государства в цифровой сфере.

Нормативную базу исследования образуют Конституция Российской Федерации, Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральный закон от 07.07.2003 № 126-ФЗ «О связи», Федеральный закон от 01.05.2019 № 90-ФЗ, Федеральный закон от 26.07.2017 № 187-ФЗ, а также Указ Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» [1-7].

Доктринальная база включает публикации, посвященные информационному и цифровому суверенитету, в том числе работы О.В. Романовской, Е.О. Гаврилова, А.А. Ефремова, Д.А. Печегина и И.В. Бородушко, в которых по-разному раскрываются пределы суверенитета государства в цифровой среде, его связь с технологической независимостью и механизмами правового регулирования [8-12].

Поскольку цифровой суверенитет находится на пересечении публичного и частного права, особое значение имеет сопоставление правовых норм с фактической архитектурой цифровых сервисов: системами связи, реестрами, платформами государственных услуг, центрами обработки данных и средствами защиты информации. Такой подход позволяет выявить, где именно возникают юридически значимые точки уязвимости и какие инструменты правового регулирования оказываются наиболее эффективными.

Исследование исходило из гипотезы, что цифровой суверенитет можно обеспечить лишь при одновременном соблюдении трех условий: наличии собственных или контролируемых государством критических цифровых ресурсов, достаточной правовой регламентации процессов обработки данных и сохранении конституционного

баланса между безопасностью, свободой информации и правом на частную жизнь.

Правовая конструкция цифрового суверенитета складывается из нескольких взаимосвязанных блоков. Первый блок связан с конституционными основами государственного суверенитета и обязанностью государства обеспечивать целостность, безопасность и независимость своего правопорядка [1]. Второй блок образуют нормы, регулирующие информационные отношения, связь и персональные данные [2]. Третий блок связан с режимом критической информационной инфраструктуры, без которого цифровой суверенитет превращается в декларацию, не подкрепленную организационными механизмами [5,7].

Федеральный закон № 149-ФЗ устанавливает общую рамку правового режима информации и информационных технологий, а Федеральный закон № 152-ФЗ формирует обязательные требования к обработке персональных данных, включая принципы законности, целевого ограничения и минимизации сведений [2,3]. В контексте цифрового суверенитета эти нормы важны не только как гарантии прав личности, но и как инструменты формирования контролируемого национального информационного пространства, в котором данные не могут произвольно перемещаться, использоваться или объединяться вне установленных правовых оснований.

Значимую роль играет Федеральный закон № 126-ФЗ «О связи», поскольку именно он задает правовые основы функционирования сетей связи, а значит, и всей инфраструктуры, через которую осуществляется доступ к цифровым сервисам, государственным информационным системам и трансграничному обмену данными [4]. В сочетании с Федеральным законом № 90-ФЗ этот акт образует правовой каркас устойчивого функционирования российского сегмента сети Интернет, предусматривая механизмы управления трафиком, координации сетевых процессов и защиты от внешних угроз устойчивости, безопасности и целостности коммуникационной среды [6].

В научной литературе цифровой суверенитет нередко связывается с понятием информационного суверенитета. Так, А.А. Ефремов показал, что «информационный суверенитет государства формируется как ответ на глобализацию и рост зависимости от транснациональных цифровых платформ», а Е.О. Гаврилов подчеркивал, что «цифровой суверенитет в условиях глобализации не может означать самоизоляцию», поскольку «государство

сохраняет включенность в международное информационное пространство» [9, 10]. Эти подходы позволяют сделать вывод о том, что цифровой суверенитет следует понимать как суверенное право государства на регулирование, а не как запрет на цифровое взаимодействие.

Важнейшим направлением регулирования является обеспечение безопасности критической информационной инфраструктуры. Федеральный закон № 187-ФЗ закрепляет специальный режим охраны значимых объектов, а Указ Президента Российской Федерации № 166 усиливает курс на технологическую независимость и преимущественное использование отечественного программного обеспечения и оборудования на значимых объектах КИИ [5,7]. В этих нормах цифровой суверенитет выражается наиболее рельефно, поскольку государство получает юридические инструменты для ограничения зависимости от иностранных решений в стратегически чувствительных сегментах.

Однако правовое регулирование цифрового суверенитета не должно сводиться к импортозамещению. При всей важности технологической автономии главным ориентиром остается человек и его конституционные права. Цифровой суверенитет, основанный исключительно на логике контроля, может привести к чрезмерному расширению наблюдения, несоразмерным ограничениям свободы информации, усилению блокировочных практик и снижению доверия к цифровой среде. Следовательно, нормативные меры в этой сфере должны оцениваться через критерии необходимости, соразмерности и правовой определенности [8].

Отдельной проблемой выступает разграничение публичного и частного контроля над цифровой инфраструктурой. Значительная часть платформ, облачных сервисов, поисковых систем и мессенджеров принадлежит частным компаниям, зачастую с трансграничной структурой управления. Это означает, что государство не может рассчитывать на цифровой суверенитет без правовых механизмов, обеспечивающих прозрачность алгоритмов, возможность локализации данных, аудита информационной безопасности и исполнения законных требований регулятора. Иначе говоря, цифровой суверенитет в современном праве невозможен без определенной степени «юридизации» цифровой архитектуры.

С практической точки зрения цифровой суверенитет проявляется в нескольких уровнях. На инфраструктурном уровне речь идет о национальных сетях связи, точках обмена трафиком, центрах обработки данных

и резервных каналах управления. На уровне данных - о режиме хранения, обработки и передачи персональных и иных чувствительных сведений. На уровне программного обеспечения - о способности государства и отечественного рынка обеспечивать базовые цифровые функции без критической зависимости от внешних поставщиков. На организационном уровне - о наличии компетентных регуляторов, механизмов межведомственного взаимодействия и процедур реагирования на компьютерные инциденты.

Романовская О.В. справедливо связывает цифровой суверенитет с более широким контекстом информационного общества, где государство вынуждено одновременно отвечать на вызовы киберугроз, ускорения обмена данными и трансформации публичного управления [8]. В этом смысле правовое регулирование цифрового суверенитета должно строиться не по модели единичного закона, а как межотраслевой комплекс норм, охватывающий конституционное, информационное, административное, гражданское и уголовное право.

Печегин Д.А. указывает на «необходимость правовых механизмов защиты цифрового суверенитета, включая регуляторные и уголовно-правовые средства, поскольку зависимость цифровой среды от внешних акторов создает не только технические, но и правонарушающие риски» [11]. Данный вывод особенно важен в условиях кибератак, дезинформации, несанкционированного доступа к данным и использования цифровых платформ в целях воздействия на общественные и государственные институты.

Отдельного внимания заслуживает вопрос о пределах государственного вмешательства. Чем более технологически сложной становится цифровая среда, тем выше риск подмены правового регулирования чисто административным контролем. Между тем цифровой суверенитет требует именно правового, а не произвольного режима: гражданин и организация должны понимать, какие данные собираются, кто ими распоряжается, на каких основаниях осуществляется ограничение доступа и как оспариваются незаконные действия операторов.

Таким образом, правовое регулирование цифрового суверенитета можно описать как систему норм, направленных на обеспечение самостоятельности государства в цифровой сфере, защиту критически важной инфраструктуры, локализацию и безопасное использование данных, а также на сохранение баланса между безопасностью и свободами личности. В этой системе юридическая защита цифровой

среды не является самоцелью: она служит инструментом устойчивого развития государства и гарантией того, что цифровизация не разрушит конституционные основы правопорядка.

Проведенное исследование позволяет сделать вывод о том, что цифровой суверенитет представляет собой самостоятельный объект правового регулирования, тесно связанный с конституционным принципом государственного суверенитета, информационной безопасностью и правами человека. Он выражает способность государства формировать и поддерживать такой режим цифровой среды, при котором ключевые инфраструктуры, данные и сервисы остаются управляемыми, защищенными и правоопределенными.

Нормативное ядро цифрового суверенитета в Российской Федерации образуют Конституция Российской Федерации, федеральные законы об информации, связи, персональных данных и безопасности критической информационной инфраструктуры, а также подзаконные акты, направленные на технологическую независимость и устойчивость национального цифрового пространства [1-7]. Вместе с тем действующее регулирование сохраняет фрагментарный характер и нуждается в концептуальном объединении.

Наиболее важным направлением дальнейшего развития законодательства является закрепление целостной дефиниции цифрового суверенитета и установление четких правил его реализации: в отношении данных, инфраструктуры, программного обеспечения, трансграничного обмена сведениями и ответственности операторов цифровых платформ. При этом любые меры по укреплению суверенитета должны оцениваться через их соответствие конституционным правам и принципу соразмерности.

Следовательно, эффективная модель правового регулирования цифрового суверенитета должна сочетать технологическую независимость, устойчивость критической инфраструктуры, защиту персональных данных и сохранение открытого, но безопасного цифрового пространства. Именно такая модель позволяет государству укреплять независимость, не подрывая правовую защищенность личности и доверие общества к цифровой трансформации.

Список литературы:

- [1] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Российская газета. 1993. 25 декабря. № 237; Российская газета. 2020. 4 июля. № 144.

[2] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. 2006. № 31. Ст. 3448.

[3] Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства Российской Федерации. 2006. № 31. Ст. 3451.

[4] Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» // Собрание законодательства Российской Федерации. 2003. № 28. Ст. 2895.

[5] Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства Российской Федерации. 2017. № 31 (часть I). Ст. 4736.

[6] Федеральный закон от 01.05.2019 № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации. 2019. № 18. Ст. 2214.

[7] Указ Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» // Официальный интернет-портал правовой информации. 30.03.2022.

[8] Романовская О.В. Право, информационное общество, цифровой суверенитет // Известия Саратовского университета. Новая серия. Серия: Экономика. Управление. Право. 2024. Т. 24, вып. 2. С. 174–183.

[9] Гаврилов Е.О. Цифровой суверенитет в условиях глобализации: философский и правовой аспекты // Вестник Кемеровского государственного университета. Серия: Гуманитарные и общественные науки. 2020. № 2. С. 146–152.

[10] Ефремов А.А. Формирование концепции информационного суверенитета государства // Право. Журнал Высшей школы экономики. 2017. № 1. С. 201–215.

[11] Печегин Д.А. Правовые механизмы защиты цифрового суверенитета государства: сравнительно-правовой аспект // Российский журнал правовых исследований. 2022. Т. 9. № 2. С. 9–20.

[12] Бородушко И.В. Технологический суверенитет России: теоретико-правовые основы, механизмы достижения // Национальная безопасность и стратегическое планирование. 2023. № 3(43). С. 86–96.

References:

[1] The Constitution of the Russian Federation (adopted by popular vote 12.12.1993 with amendments approved during the all-Russian vote 01.07.2020) // Rossiyskaya Gazeta. 1993. December 25. № 237; Russian newspaper. 2020. July 4th. № 144.

[2] Federal Law of 27.07.2006 No. 149-FZ “On Information, Information Technologies and Information Protection” // Collection of Legislation of the Russian Federation. 2006. № 31. Art. 3448.

[3] Federal Law of 27.07.2006 No. 152-FZ “On Personal Data” // Collection of Legislation of the Russian Federation. 2006. № 31. Art. 3451.

[4] Federal Law of 07.07.2003 No. 126-FZ “On Communications” // Collection of Legislation of the Russian Federation. 2003. № 28. Art. 2895.

[5] Federal Law of 26.07.2017 No. 187-FZ “On the Security of the Critical Information Infrastructure of the Russian Federation” // Collection of Legislation of the Russian Federation. 2017. No. 31 (Part I). Art. 4736.

[6] Federal Law of 01.05.2019 No. 90-FZ “On Amendments to the Federal Law “On Communications” and the Federal Law “On Information, Information Technologies and Information Protection” // Collection of Legislation of the Russian Federation. 2019. № 18. Art. 2214.

[7] Decree of the President of the Russian Federation of 30.03.2022 No. 166 “On measures to ensure the technological independence and security of the critical information infrastructure of the Russian Federation” // Official Internet portal of legal information. 30.03.2022.

[8] Romanovskaya O.V. Law, Information Society, Digital Sovereignty // Izvestia Saratov University. New series. Series: Economics. Management. Right. 2024. Vol. 24, no. 2. S. 174-183.

[9] Gavrilov E.O. Digital sovereignty in the context of globalization: philosophical and legal aspects // Bulletin of Kemerovo State University. Series: Humanities and Social Sciences. 2020. № 2. S. 146-152.

[10] Efremov A.A. Formation of the concept of information sovereignty of the state // Law. Journal of the Higher School of Economics. 2017. № 1. S. 201-215.

[11] Pechegin D.A. Legal mechanisms for protecting the digital sovereignty of the state: comparative legal aspect // Russian Journal of Legal Research. 2022. VOL. 9. № 2. S. 9-20.

[12] Borodushko I.V. Technological sovereignty of Russia: theoretical and legal foundations, mechanisms of achievement // National security and strategic planning. 2023. № 3(43). S. 86-96.