УДК 34.01, 342 DOI: 10.31249/iajpravo/2024.02.13

АЛФЕРОВА Е.В.[1] ГОСУДАРСТВЕННЫЙ СУВЕРЕНИТЕТ В ИНФОРМАЦИОННОМ (ЦИФРОВОМ) ПРОСТРАНСТВЕ: ДОКТРИНАЛЬНЫЕ И ЗАКОНОДАТЕЛЬНЫЕ ПОДХОДЫ

Аннотация. Понятие государственного суверенитета включает понимание таких составляющих его элементов, как верховная власть и территория. На основе анализа новых публикаций по суверенитету и киберпространству в данном обзоре показано, как эти ключевые свойства государства действуют в Интернете. Дебаты об информационном (цифровом) суверенитете в киберпространстве отражают разные идеи и практики в этом вопросе. Ученые рассматривают роль и значение суверенитета государства в определении правового статуса киберпространства. Утверждается, что концепция цифрового суверенитета не размывает классическое понятие «суверенитет государства», а лишь отражает вызовы независимости государства, исходящие из различных источников международной конкуренции. Государственный суверенитет признается в качестве основы регулирования межгосударственных отношений в ИКТ-среде.

Ключевые слова: государственный суверенитет; цифровой (информационный) суверенитет; цифровое государство; конституционно-правовое регулирование.

ALFEROVA E.V. State sovereignty in the information (digital) space: doctrinal and legislative approaches

Abstract. The concept of State sovereignty includes an understanding of such constituent elements as the supreme power and terri-

[1] *Алферова Елена Васильевна*, ведущий научный сотрудник отдела правоведения ИНИОН РАН.

tory. Based on the analysis of new publications on cyberspace and sovereignty, this review shows how these key properties of the state operate on the Internet. The debate on information (digital) sovereignty in cyberspace reflects different ideas and practices on this issue. Scientists consider the role and importance of state sovereignty in determining the legal status of cyberspace. It is argued that the concept of digital sovereignty does not dilute the classical concept of «state sovereignty», but only reflects the challenges to state independence emanating from various sources of international competition. State sovereignty is recognized as the basis for regulating interstate relations in the ICT environment.

Keywords: state sovereignty; digital (information) sovereignty; digital state; constitutional and legal regulation.

Для цитирования: Алферова Е.В. Государственный суверенитет в информационном (цифровом) пространстве: доктринальные и законодательные подходы // Социальные и гуманитарные науки. Отечественная и зарубежная литература : ИАЖ. Сер. Государство и право. – 2024. – № 2. – С. 171–186. – DOI: 10.31249/iajpravo/2024.02.13

Введение

Почти три десятилетия назад, в 1996 г., Джон Перри Барлоу разработал Декларацию независимости киберпространства, в которой провозглашается идея отсутствия суверенитета государства в данной сфере[1]. Суверенитет традиционно был противоречивой юридической и политической категорией, и до сих пор не прекращаются дискуссии о суверенитете в киберпространстве. Глобализация и цифровая технификация, как замечает профессор М. Роблес-Каррильо из Гранадского университета (Испания), представляют собой особенно серьезную проблему для суверенитета. С самого начала цифровая сфера представлялась средой, вряд ли подходящей для осуществления суверенитета. Она не имеет границ и пересекает остальные физические пространства, стирая эффект географических границ. Несмотря на время, прошедшее с момента его возникновения, вопрос о суверенитете в цифровом мире по-

[1] См.: Barlow J.P. Declaration on the Independence of Cyberspace. – 1996. – URL: https://www.eff.org/cyberspace-independence (дата обращения: 11.01.2024).

прежнему вызывает споры. В 2020 г. М.Л. Мюллер написал статью «Против суверенитета в киберпространстве» (Mueller M.L. «Against Sovereignty in Cyberspace»), в 2021 г. К.Дж. Хеллер опубликовал статью «В защиту чистого суверенитета в киберпространстве» (Heller K.J. «In Defense of Pure Sovereignty in Cyberspace»). По мере продолжения этих дискуссий появилась новая концепция цифрового суверенитета. Однако, по мнению М. Роблес-Каррильо, «нет свидетельств существенных изменений понятия суверенитета, за исключением того факта, что ряд стран и организаций продвигают управленческие подходы с точки зрения множественных субъектов: “суверенитет и государственная власть изменены, но не уничтожены”» [13, p. 673–674].

В научных исследованиях и в официальных документах появились близкие по смыслу понятия «информационный суверенитет», «цифровой суверенитет», «сетевой суверенитет», «компьютерный суверенитет», «технологический» и др. Однако не существует единого или превалирующего определения цифрового суверенитета, нет и консенсуса по поводу самого термина; в литературе эти слова часто используются как альтернативные, объединяющие или взаимозаменяющие. Высказывается мнение, что их нельзя использовать как синонимы, так как каждый представляет «один из аспектов единой, более широкой концепции цифрового суверенитета» [11].

По словам Ю. Поль и Т. Тиля (Берлинский Центр социальных наук), понятие цифрового суверенитета «стало гораздо более всеохватывающим и относится не только к вопросам коммуникации в Интернете, но и к более широким вопросам цифровой трансформации обществ» [12]. Растущий интерес к понятию «цифровой суверенитет» объясняется учеными отчасти технологическими причинами (рост значимости облачных технологий), а также разоблачениями фактов государственного и корпоративного шпионажа [5, с. 63].

Китайский профессор В. Гонг определяет «информационный суверенитет»[1] через внутреннюю и внешнюю составляющие.

[1] Не исключая возможного различия с точки зрения содержательных характеристик цифрового и информационного суверенитета, представляется, что в рамках формирования общего доктринального видения данной проблемы эти понятия в настоящей работе рассматриваются в качестве синонимичных.

Внутреннее понимание этого термина заключается в роли высшей государственной власти в формулировании и реализации информационной политики и поддержании информационного порядка в стране, внешнее – в полном юридическом равенстве государств и их независимости от внешнего контроля при производстве и использовании информации [10].

С начала XXI в. в России опубликовано несколько десятков диссертационных исследований по теме «цифровой (информационный) суверенитет», в том числе по теории права и государства, международному и конституционному (государственному) праву, информационному праву[1]. Опубликованы многочисленные монографические и другие научные и учебные издания[2].

Развитие концепции информационного суверенитета государства. Проблематика государственного суверенитета в информационной сфере в правовой науке активно ведется с 1980-х годов. А.А. Ефремов выделяет три периода развития концепции государственного суверенитета в информационном пространстве (информационного суверенитета государства):

[1] Список ряда диссертационных работ и других исследований см.: Ефремов А.А. Государственный суверенитет в условиях цифровой трансформации // Правоведение. – 2019. – Т. 63, № 1. – С. 48–48; Он же. Защита государственного суверенитета РФ в информационном пространстве. – Москва, 2020. – 128 с.

[2] См., напр.: Государство и право в новой цифровой реальности / РАН. ИНИОН ; под ред. И.А. Умновой-Конюховой, Д.А. Ловцова. – Москва, 2020. – 259 с.; Ефремов А.А. Защита государственного суверенитета РФ в информационном пространстве. – Москва, 2020. – 128 с.; Черногор Н.Н., Пашенцев Д.А., Залоило М.В. Концепция цифрового государства и цифровой правовой среды / Ин-т законодательства и сравн. правоведения при правительстве РФ. – Москва, 2021. – 244 с.; Право, цифровые технологии и искусственный интеллект / РАН, ИНИОН ; отв. ред. Е.В. Алферова. – Москва, 2021. – 267 с.; Умнова-Конюхова И.А., Алферова Е.В., Алешкова И.А. Цифровое развитие и права человека. – Москва, 2021. – 174 с.; Цифровая трансформация и государственное управление / А.С. Емельянов, А.А. Ефремов, А.В. Калмыкова [и др.] ; ред. кол.: Л.К. Терещенко, А.С. Емельянов, Н.А. Поветкина. – Москва, 2022. – 224 с.; Права человека в информационной сфере в условиях цифровизации / Н.С. Волкова, А.С. Емельянов, А.А. Ефремов [и др.] ; отв. ред. Л.К. Терещенко. – Москва, 2023. – 244 с.; Жарова А.К. Правовое регулирование создания и использования информационной инфраструктуры в Российской Федерации. – Москва , 2023. – 301 с.; и др.

– *1980-е годы* – выявление соотношения категорий «свобода информации» и «национальный суверенитет», обусловленное развитием трансграничного информационного обмена посредством радио-, теле- и спутникового вещания. Формирование правовой теории информационного пространства, киберпространства только начинается;

– *1990-е годы* – развитие Интернета как международной компьютерной сети. Данный этап характеризуется появлением работ, рассматривающих Интернет как угрозу государственному суверенитету;

– *2010-е годы – настоящее время* – появление концепции суверенитета данных (data sovereignty), связанной с формированием в ряде стран законодательства, предусматривающего локализацию персональных и иных данных в рамках информационной инфраструктуры исключительно данного государства [2, с. 66–72].

Автор выделяет также четвертый этап, обусловленный цифровизацией. Начальный его период он связывает с принятием в мае 2015 г. Еврокомиссией Стратегии единого цифрового рынка ЕС (Digital Single Market (DSM) Strategy), в июне 2016 г. Организацией экономического сотрудничества и развития цифровой экономики – Канкунской декларации: «Инновации, рост и социальное благополучие» и в декабре 2016 г. – Цифровой повестки Евразийского экономического союза, разработанной Евразийской экономической комиссией и подписанной главами государств ЕАЭС и др. [там же].

Следуя нарративу, отличному от понимания цифрового суверенитета, принцип суверенитета, по мнению М.М. Роблес-Каррильо, выражается через его утверждение в киберпространстве несколькими различными способами. Во-первых, принцип киберсуверенитета укрепился в качестве модели управления, продвигаемой рядом стран и международных организаций, в первую очередь Китаем, Россией и Шанхайской организацией сотрудничества, а также в качестве альтернативной модели был поддержан Соединенными Штатами, странами Большой семерки и Евросоюзом. Во-вторых, принцип суверенитета в отношении инфраструктур, сетей и систем, расположенных на территории государства, был принят огромным большинством стран, а также согласован в рамках работы Групп правительственных экспертов и Рабочей

группы открытого состава, утвержденных Генеральной Ассамблеей ООН для обсуждения прогресса в сфере ИКТ и международной безопасности. В-третьих, ряд государств ввели принцип киберсуверенитета при создании своего собственного цифрового пространства с целью обособиться и отделиться от общей цифровой зоны. Так, Китай создал так называемую «Цифровую стену», а Российская Федерация – Яндекс и Рунет [13, p. 677].

Фактически за этим процессом последовательного утверждения суверенитета в киберпространстве стоит несколько уровней мотивации. Государства провозглашают его разными способами и с разной степенью интенсивности. Три главные из них определили А. Чандер (Джорджтаунский университет), и Х. Сан (Гонконгский университет). Правительства выступают за цифровой суверенитет в целях защиты своего населения, например: стремятся удалить материалы, считающиеся незаконными в данной стране (1); развивают собственную цифровую экономику (2); контролируют поведение своих граждан, например, ограничиваютсвободу информации (3).

Попытки уточнить, приспособить суверенитет государства к каким-либо аспектам государственной политики (военной, экономической, в области культуры и др.), по мнению профессора А.Я. Капустина, нельзя рассматривать иначе как стремление привлечь внимание к угрозам государственному суверенитету в различных сферах международных отношений. С его точки зрения, концепция цифрового суверенитета не размывает классического понятия «суверенитет государства», а лишь отражает вызовы независимости государства, исходящие из различных источников международной конкуренции [4, с. 107]. За четыре столетия, истекшие со времени появления доктрины суверенитета государства в XVI в., этот институт значительно трансформировался, однако его сущностные характеристики оставались неизменными – верховенство государства в пределах границ своей территории и его независимость на международной арене [там же].

«Цифровое государство» и три направления концептуальной роли суверенитета в определении правового статуса ИКТ-среды, или киберпространства. Процессы информатизации общества не обошли стороной и его основной институт – государство. В научной юридической, политологической и экономической

литературе обсуждаются концепции «цифрового государства», «цифровой экономики», «цифрового управления», «цифрового судопроизводства» и др. Авторы книги «Концепция цифрового государства и цифровой правовой среды» Н.Н. Черногор, Д.А. Пашенцев, М.В. Залоило определяют три подхода к определению понятия «цифровое государство». Первый – инструментально-технологический, основанный на идее взаимодействия трех ветвей власти государства и муниципальной власти и населения на основе ИКТ. Второй – организационно-управленческий, описывающий этот феномен как новую форму информационных взаимоотношений между государство, государством и бизнесом, государством и гражданами. Третий подход – процедурно-процессуальный – продвигает идею новой формы демократии, цифровой или электронной, обеспечивающей максимальное участие граждан в государственном управлении [8, с. 14–15].

В предложенном авторами понимании понятия цифрового государства речь идет не о замене сущности категории «государство», а о формировании новой формы его взаимодействия с населением страны. Иными словами, сама «цифра», определяемая как информационно-коммуникативные технологии (ИКТ), еще не приобрела качества носителя власти, а является скорее инструментом ее реализации. По мнению А.Я. Капустина, в данном случае суверенитет понимается в его классическом смысле как свойство государства, а не цифровой формы взаимодействия государства с обществом [4, с. 102].

Профессор А.Я. Капустин предлагает условно выделить три направления концептуального восприятия роли суверенитета в определении правового статуса ИКТ-среды, или киберпространства, а также признания государственного суверенитета в качестве основы регулирования межгосударственных отношений в ИКТ-среде [4, с. 103–105].

Первый подход – исключительно нигилистический, его представители отрицают саму возможность признания суверенитета государства в киберпространстве. Это сторонники так называемой идеи кибериключительности, предлагавшие признать киберпространство полностью свободным от суверенитета государства. Ключевая идея – киберпространство должно развивать собственную правовую систему, основанную на концепции саморегулирования.

Представители *второго подхода* признают значение государственного суверенитета для международно-правового регулирования статуса киберпространства, однако более практичным и реальным считается использование в киберпространстве не принципа суверенитета, а понятия юрисдикции государства, которая характеризует способность государства применять принуждение. Государство может осуществлять юрисдикцию над киберинфраструктурой, расположенной на его территории и над его гражданами, когда они вовлечены в кибердеятельность на основе двух принципов: персонального (гражданство) или территориального (на своей территории или экстерриториально). Указанные принципы получили подтверждение в международной и национальной судебной практике. Не отрицая значения юрисдикции для обеспечения и защиты национальных интересов, ученый замечает, что «редукция понимания роли суверенитета государства в киберпространстве до признания лишь возможности реализации им юрисдикционных полномочий не создает твердых гарантий безопасности отдельного государства от таких серьезных угроз, как причинение злонамеренного ущерба или разрушения критически важной инфраструктуры и иных масштабных нарушений жизнедеятельности» [4, с. 106].

Как отмечает А.Я. Капустин, идею «генеративной модели минимального суверенитета киберпространства» выдвинул Т. Ву. С точки зрения этого китайского исследователя, в будущем эта модель «должна спровоцировать необходимые изменения правового регулирования». Смысл ее, или замысел в том, что она «повлечет за собой процесс, посредством которого нормы и правила киберпространства могут стать уважаемыми значительным числом государств» [4, с. 106–107].

Третий подход, с точки зрения автора, более реалистичный. Сторонники этого подхода признают растущую заинтересованность государств в укреплении суверенитета в киберпространстве, особенно в свете непрекращающихся обвинений во вмешательстве во внутренние дела государств с использованием ИКТ. Реализм подобной позиции, по мнению А.Я. Капустина, объясняется практической направленностью исследований, опирающихся на официальные позиции государств, особенно занимающих лидирующие позиции в сфере ИКТ, а также желанием не ограничиваться

научным конструированием, а направить усилия на выработку рекомендаций по международно-правовому регулированию статуса киберпространства и мер, обеспечивающих суверенитет государств. В их числе автор отмечает позицию Х. Мойнихан, которая, следуя классическому пониманию суверенитета государства, рассматривает его как принцип международного права, который включает совокупность суверенных прав: право государства на территориальный суверенитет, право на независимость государственной власти и идею равенства государств в международном порядке (внешний суверенитет). Отсюда следует, что осуществление каким-либо государством своей власти на территории другого государства без его согласия представляет собой нарушение суверенитета этого последнего государства [4, с. 107–108]. При этом приводятся позиции государств, опубликованные в 2019–2020 гг. (Нидерланды, Франция, Австрия, Чешская Республика и Иран), считающих, что несанкционированное кибернападение одного государства на объекты киберпространства другого государства может, при определенных обстоятельствах, привести к нарушению государственного суверенитета. Подобная позиция рассматривается как дополнительное свидетельство того, что государства не отказались от желания сохранить свой суверенитет в киберпространстве [там же].

Интересна в связи с этим позиция Н. Цагуриаса, председателя отделения международного и европейского права Университета Шеффилда (Великобритания), исследующего в своей статье вопрос соотношения киберпространства и суверенитета [14]. Автор пытается ответить на два вопроса: может ли киберпространство быть объектом суверенитета и может ли оно быть суверенным? По его мнению, киберпространство – это «всемирная территория внутри информационного пространства. Оно организовано с помощью электроники и электромагнетического спектра для создания, хранения, изменения, обмена и использования информации через взаимозависимые и взаимосвязанные сети с использованием ИКТ» [14, p. 15]. Суверенитет же в международно-правовом значении тесно связан с территорией. Но поскольку суть суверенитета не в территории, а во власти, он может распространяться не только за пределы какой-либо территории, но и на внетерриториальные сущности. Правовым наполнением суверенитета государства явля-

ется его правомочия, которые оно реализует в отношении киберструктуры, расположенной на его территории, и над гражданами, вовлеченными в кибердеятельность, а также над негражданами, находящимися на его территории. Государство осуществляет юрисдикцию над информацией, циркулирующей в гиперпространстве, в точке приема или в точке доставки, а также над информацией, проходящей по каналам и проводам, подпадающим под его юрисдикцию. Веб-адреса также находятся в пределах юрисдикции государства, поскольку они зарегистрированы в конкретной стране. Иными словами, государство может осуществлять юрисдикцию над киберпространством и кибердеятельностью на национальной и территориальной основах. Следовательно, утверждает Н. Цагуриас, юрисдикция и, соответственно, суверенитет государства могут увеличиваться. Применительно к киберпространству это означает, что, если гражданин одного государства совершил киберпреступление на территории другого государства, первое сохраняет свою юрисдикцию над ним. Более того, в соответствии с принципом пассивной национальности, признаваемым многими государствами, в частности, по отношению к актам терроризма, государство может экстратерриториально распространить свою юрисдикцию на своих граждан в случаях, когда они стали жертвами преступления. Расширение юрисдикции возможно и случаях, когда кибердеятельность приводит к последствиям на территории государства. Государство может заявить о своей юрисдикции в ситуации, когда под угрозой оказываются его национальные интересы, вне зависимости от того, где и кем осуществлялась угрожающая этим интересам деятельность. Речь идет в первую очередь о кибершпионаже. Государство вольно заявлять свою юрисдикцию, «его право на осуществление юрисдикции опирается на его суверенитет» [14, p. 15–23].

Таким образом, по мнению Н. Цагуриаса, наблюдаются, с одной стороны, территоризация киберпространства и деятельности в нем, с другой – детерриторизация суверенитета[1].

[1] Подробнее см.: Цагориас Н. Правовой статус [реф.] // Государство и право в новой информационной реальности : сб. науч. тр. / РАН, ИНИОН, Отд. правоведения, РГУП, Каф. информационного права, информатики и математики ; отв. ред. Е.В. Алферова, Д.А. Ловцов. – Москва, 2018. – С. 112–118. – Реф. ст.:

Конституционно-правовые характеристики цифрового (информационного) суверенитета. Российские ученые-правоведы А.В. Даниленков, С.В. Нарутто, С.Ю. Колмаков, И.М. Япрынцев считают, что юридическая доктрина не выработала единого комплексного подхода к пониманию цифрового (информационного) суверенитета, которое охватывало бы всю специфику субъектов и особенностей правоотношений в информационно-коммуникационной сфере, возникающих в связи с осуществлением публично-властных полномочий государства в этой области [1, с. 157; 6, с. 15]. Тем не менее существующий теоретический и нормативный материал позволяет выделить конституционно-правовые характеристики информационного суверенитета, которые дают возможность создавать необходимые механизмы его реализации и защиты. Так, А.К. Жарова полагает, что по своим общим нормативно-правовым характеристикам информационный суверенитет является составной частью суверенитета государственного [4, с. 28–29]. Несколько иными словами, но аналогично А.А. Ефремов определяет информационный суверенитет как государственный суверенитет в информационном пространстве [2]. Есть и другие мнения, но они не меняют сути государственного суверенитета. Так, Э.В. Талапина полагает, что нет необходимости дробления категории «суверенитет», и целесообразно применять единое понятие государственного суверенитета ко всем сферам его реализации, включая информацию и информационные технологии [7, с. 60–67]. Однако объективно складывающиеся общественные отношения в информационно-цифровой сфере, полагают ученые, предопределяют необходимость доктринального осмысления изменения суверенитета и гарантий его реализации [6, с. 15–16].

В доктрине цифрового (информационного) суверенитета выделяются наиболее важные компоненты, с которыми связывается гарантирование информационной безопасности государства: поисковая система, социальные сети, операционная система и программное обеспечение, микроэлектроника, сетевое оборудование, национальный сегмент сети Интернет, платёжная система, собственные средства защиты, криптографические алгоритмы и протоко-

Tsagourias N. The legal status of cyberspace // Research handbook on international law and cyberspace. – St. Louis : Edward Elgar publ., 2016. – P. 13–29.

лы, навигационная система. В дополнение к указанным в качестве определяющих информационный суверенитет относят и другие критерии, как то разработку и использование собственных ИТ-решений в различных сферах общественных отношений; возможность автономного функционирования цифрового пространства; наличие базовых и продвинутых навыков работы с цифровыми технологиями как у рядовых граждан, так и у профессиональных ИТ-специалистов, и т.д. [6, с. 15–16]. Естественно, что такие важные области цифровых (информационных) отношений подвергаются правовому регулированию не только на международном уровне, но и внутреннем, в частности, в конституционном законодательстве государств. Так, в Конституции РФ в результате конституционных поправок 2020 г. появилось положение, содержащее обязательство Российской Федерации обеспечивать защиту своего суверенитета (ч. 2.1 ст. 67). Сам факт конституционного закрепления данной нормы не указывает на отсутствие этого обязательства государства до указанной поправки, тем не менее само по себе такое регулирование актуализирует стремление государства в сфере гарантирования и обеспечения суверенитета во всех сферах его осуществления. Кроме того, была уточнена сфера полномочий публичной власти в связи с продолжающейся цифровизацией государства. Так, п. «и» ст. 71 информация, информационные технологии и связь отнесены к исключительному ведению Российской Федерации, что предполагает в первую очередь регулятивную компетенцию федерального уровня публичной власти, с тем, чтобы нормативно установить основания и порядок реализации государством и иными субъектами своих прав, в том числе в сфере реализации информационного суверенитета [там же].

Общие тенденции нормативно-правового регулирования информационного (цифрового) суверенитета в России. Общей тенденцией нормативно-правового регулирования информационного суверенитета является факт закрепления тех или иных его элементов в подзаконных, нередко стратегически направленных нормативных актах. Так, например, в Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента РФ от 02.07.2021 № 400, развитие безопасного информационного пространства признано одним из национальных интересов Российской Федерации на современном этапе (п. 25), а информаци-

онная безопасность – стратегическим национальным приоритетом (п. 26). При этом в принятой ранее Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента РФ от 05.12.2016 № 646, целями обеспечения информационной безопасности государства объявлялись достижение и поддержание информационного суверенитета.

В контексте рассмотрения вопроса о соотношении безопасности (на различных уровнях) и обеспечения информационного суверенитета интерес представляет подход, закрепленный в Стратегии обеспечения информационной безопасности государств – участников Содружества Независимых Государств, утвержденной решением Совета глав правительств СНГ 25.10.2019 г. В этой Стратегии определены основные угрозы информационной безопасности; к ним, в том числе, отнесены посягательства на информационный суверенитет государств – участников СНГ, на их право самостоятельно владеть, пользоваться и распоряжаться своими информационными ресурсами, а также деструктивное информационное воздействие на личность, общество, государственные институты и их информационную инфраструктуру, наносящее ущерб национальным интересам государств и др. При таком подходе информационный суверенитет выступает гарантом информационной безопасности, которая должна обеспечиваться как на государственном уровне, так и на личностно-общественном [6, с. 16–17].

Отдельные элементы цифрового суверенитета нормативно отражены и в других нормативных правовых актах. Например, в Указе Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» говорится о технологическом суверенитете как средстве обеспечения необходимого уровня самостоятельности Российской Федерации в области искусственного интеллекта, в том числе посредством преимущественного использования отечественных технологий искусственного интеллекта и технологических решений, разработанных на основе искусственного интеллекта; в Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг., утвержденной Указом Президента РФ от 09.05.2017 № 203, подчеркивается необходимость гарантировать суверенное право государства определять информационную, технологическую и экономическую политику в национальном сегменте сети Интернет; в Стратегии

научно-технологического развития Российской Федерации, утвержденной Указом Президента РФ от 01.12.2016 (ред. от 15.03.2021), предусматривается, что риски и угрозы в информационной сфере становятся существенным барьером, препятствующим долгосрочному росту благосостояния общества и укреплению суверенитета России.

По мнению ученых, фрагментарность нормативного регулирования информационного суверенитета во многом предопределена отсутствием системности в осмыслении данной категории на научно-доктринальном уровне. Регулирование отдельных аспектов суверенных полномочий в информационно-цифровой среде, отчасти противоречивое, не позволяет говорить о формировании в Российской Федерации конституционно-правовых основ осуществления информационного суверенитета и предполагает необходимость пересмотра выработанных подходов государственной политики в этой сфере [6, с. 19].

Внесение поправок в Конституцию РФ позволяет несколько по-иному взглянуть на этот фундаментальный вопрос. Новая редакция в 2020 г. пунктов «и», «м» ст. 71 Конституции РФ, определяющих предметы федерального ведения в системе разделения полномочий между органами государственной власти Российской Федерации и субъектов РФ, отражают принципиально важные конституционные изменения роли государства в информационных отношениях в условиях цифровизации[1]. Суть этих поправок состоит в том, что в ведении Российской Федерации теперь находятся не только оборона, границы, недра и так далее, но и информационные технологии и оборот цифровых данных. Новеллы п. «и» и «м» ст. 71 Конституции РФ становятся отправной точкой для реализации в российском законодательстве концепции цифрового суверенитета государства и личности.

[1] Подробнее см.: Алферова Е.В. Цифровые новеллы Конституции Российской Федерации: взгляд ученых-юристов // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 4: Государство и право. – 2023. – № 4. – С. 92–108.

Заключение

Оценивая значение концепции суверенитета государства в современных условиях цифровизации, российские ученые признают необходимость ее доктринального обоснования и конституционно-правового закрепления. Суверенитет и юрисдикция государства остаются неотъемлемыми его свойствами, поэтому появление цифровой среды не может пошатнуть суверенитет. В этом смысле концепция защиты государственного суверенитета в информационном (цифровом) пространстве выглядит вполне соответствующей классическому ее пониманию в отечественной правовой литературе (А.Я. Капустин, А.А. Ефремов и др.). Однако этот вывод не означает, что не могут встречаться разногласия и различные интерпретации понятия суверенитета в киберпространстве. Задача юридической науки состоит в том, чтобы преодолевать встречающиеся разночтения в понимании терминов, понятий и категорий, обусловленных принадлежностью к различным правовым системам и традициям.

Таким образом, анализ научных дискуссий по рассматриваемой теме позволяет согласиться с утверждением, что цифровой суверенитет не является «онлайн-версией» государственного суверенитета, он не заменяет и не отменяет эту политико-правовую категорию и не расширяет принципа суверенитета.

Список литературы

1. Даниленков А.В. Государственный суверенитет Российской Федерации в информационно-телекоммуникационной сети интернет // Lex russica. – 2017. – № 7 (128). – С. 155–165.
2. Ефремов А.А. Информационно-правовой механизм обеспечения государственного суверенитета Российской Федерации : дис… д-ра. юрид. наук. – Москва, 2020. – 418 с. – URL: https://izak.ru/upload/iblock/0b5/EfremovAA_info_suverenitet_disser_IZISP_sentyabr2020_kor.pdf?ysclid=lsumg4v1dh64481851 (дата обращения: 20.02.2024).
3. Жарова А.К. Обеспечение информационного суверенитета Российской Федерации // Юрист. – 2021. – № 11. – С. 28–33.
4. Капустин А.Я. Суверенитет государства в киберпространстве: международно-правовое измерение // Журнал зарубежного законодательства и сравнительного правоведения. – 2022. – Т. 18, № 6. – С. 99–108.

5. Кутюр С., Тоупин С. Что означает понятие «суверенитет» в цифровом мире? // Вестник международных организаций. – 2020. – Т. 1, № 4. – С. 48–69. – На рус. языке.
6. Нарутто С.В., Колмаков С.Ю., Япрынцев И.М. Информационный суверенитет: конституционно-правовые основы в условиях развития цифрового государства // Образование и право. – 2022. – № 10. – С. 14–22.
7. Талапина Э.В. Государственный суверенитет в информационном пространстве: новые задачи права // Государство и право. – 2018. – № 5. – С. 60–67.
8. Черногор Н.Н., Пашенцев Д.А., Залоило М.В. Концепция цифрового государства и цифровой правовой среды : монография / Ин-т законодательства и сравн. правоведения при правительстве РФ. – Москва, 2021. – 244 с.
9. Chander A., Sun H. Sovereignty 2.0. – 2021. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3904949 (дата обращения: 11.01.2024).
10. Gong W. Information Sovereignty Reviewed // Intercultural Communication Studies. – 2005. – Vol. 14, N 1. – P. 119–135.
11. Europe's Quest for Digital Sovereignty: GAIA-X as a Case Study / Istituto Affari Internazionali (IAI). – Roma, 2021. – URL: https://www.iai.it/en/pubblicazioni/europes-quest-digital-sovereignty-gaia-x-case-study (дата обращения: 11.01.2024).
12. Pohle J., Thiel T. Digital sovereignty // Internet Policy Review. – 2020. – N 9 (4). – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4081180 (дата обращения: 11.01.2024).
13. Robles-Carrillo M. Sovereignty vs. digital sovereignty // Journal of Digital Technologies and Law. – 2023. – N 1 (3). – P. 673–690. – URL: https://doi.org/10.21202/jdtl.2023.29 (дата обращения: 11.01.2024).
14. Tsagourias N. The legal status of cyberspace // Research handbook on international law and cyberspace. – St. Louis : Edward Elgar publ., 2015. – P. 13–29.